Installation and Operation Manual

IP-DECT Base Station and IP-DECT Gateway (software version 5.0.x)

15 February 2012 / Ver. H

1 Introduction 1
1.1 Abbreviations and Glossary 2
2 Description 3
2.1 IPBS1 3
2.1.1 IPBS1 with Internal Antenna 3
2.1.2 IPBS1 with External Antennas 5
2.2 IPBS2 6
2.2.1 IPBS2 with Internal Antenna 6
2.2.2 IPBS2 with External Antennas 8
2.3 IPBL 10
2.3.1 Overview 10
2.3.2 Power Supply 10
2.3.3 LED indication 11
2.4 DECT Base Station (BS3x0) 13
2.4.1 DECT Base Station 13
2.5 DB1 15
2.5.1 DB1 with Internal Antenna 15
2.5.2 DB1 with External Antennas 17
2.6 AC-adapter 18
3 Safety Instructions 19
3.1 Protection Against Electrostatic Discharge (ESD) 19
3.1.1 ESD Handling 19
3.2 Safety Aspects 20
3.2.1 IP-DECT Base Station 20
3.2.2 DECT Base Station BS3x0 and TDM-DECT Base Station DB1 20
3.2.3 IP-DECT Gateway (IPBL) 20
3.3 Regulatory Compliance Statements (EU/EFTA only) 20
3.4 Regulatory Compliance Statements (USA and Canada only) 20
4 IP Security 22
4.1 IP Security Terminology 22
4.1.1 SSL/TLS 22
4.1.2 Public Key Infrastructure 22
4.1.3 Cryptography 22
4.2 Introduction to IP Security in IP-DECT 24
4.2.1 Secure Web Access (https) 24
4.2.2 TLS Certificates 24
4.3 IP-DECT Administrative Functions 26
4.3.1 Configuration - HTTP 26
4.3.2 Configuration - Certificates 26
4.3.3 Configuration - SIPS 26

4.3.4 Configuration - Secure RTP 26

5 Installation of the Base Station 27

5.1 Base Station Cabling 27

5.2 Install the Base Station 27

5.2.1 Fix the Mounting Bracket to a Wall 27

5.2.2 Fix the Mounting Bracket to a Ceiling 28

5.2.3 Fix the Mounting Bracket to a Pole or Beam 28

5.2.4 Use the Cable Ducts for IPBS1 29

5.2.5 Connect External Antennas (only IPBS2 and DB1) 30

5.2.6 Secure the Cable 32

5.2.7 Pinning 32

5.2.8 Connect the Base Station Cables 33

5.2.9 Mount the Base Station 33

5.3 Power the Base Station 34

5.3.1 Power the IPBS over Ethernet 34

5.3.2 Power the BS3x0 and DB1 over Express Powering Pair (EPP) and data pairs 34

5.3.3 Power the Base Station with a Local Power Supply 34

6 Installation of the IPBL 36

6.1 Install the IPBL 36

6.2 Pin the IPBL Cable 38

6.2.1 Synchronization Cable 38

6.2.2 RFP Cable 39

6.2.3 LAN Cable 39

6.3 Power the IPBL 40

6.3.1 110/230 VAC 40

6.3.2 48 VDC 41

7 Configuration 42

7.1 Requirements 42

7.1.1 Web Browser Requirements 42

7.2 Access the GUI 42

7.2.1 Determine the IP Address 43

7.2.2 Change the Default Password 44

7.3 GUI Web Access 46

7.3.1 Login Page 46

7.3.2 Access Levels 46

7.3.3 Auditors 46

7.3.4 User Administrators 46

7.3.5 System Administrators 47

7.4 Configure the Mobility Master 50

7.5 Configure the Standby Mobility Master 50

7.6 Configure the Pari Master 51
7.7 Configure the Standby Pari Master 52
7.8 Configure the Master 52
7.9 Configure the Standby Master 53
7.10 Plug and Play Configuration 54
7.11 Configure the Radio 54
7.12 Configure Deployment 54
7.13 Add Users 55
7.13.1 Anonymous Registration 56
7.13.2 Individual Registration 57
7.13.3 Easy Registration 58

8 Operation 60

8.1 General 60
8.1.1 Name the IPBS/IPBL 60
8.1.2 Change User Name and Password 60
8.1.3 Centralized Management of Administrator/Auditor Accounts Using Kerberos 61
8.1.4 Configure Automatic Firmware Update 68
8.1.5 Configure the NTP Settings 68
8.1.6 Configure Logging 69
8.1.7 Configure the HTTP settings 71
8.1.8 Configure the HTTP Client settings 72
8.1.9 SNMP 72
8.1.10 Certificates 73
8.1.11 License 79
8.2 LAN 79
8.2.1 Set DHCP Mode 79
8.2.2 Set a Static IP Address 80
8.2.3 Dynamic IP address via DHCP 80
8.2.4 Link 80
8.2.5 Configure VLAN 80
8.2.6 View LAN Statistics 81
8.2.7 Deactivate LAN Port (only for IPBL) 81
8.3 IP 81
8.3.1 Configure IP Settings 81
8.3.2 Routing 82
8.4 LDAP 82
8.4.1 Configure LDAP Server 82
8.4.2 Check LDAP Server Status 82
8.4.3 Configure LDAP Replicator 83
8.4.4 Check LDAP Replicator Status 88

8.4.5 Expert tool 88
8.5 DECT 88
8.5.1 Change System Name and Password 89
8.5.2 Set Subscription Method 89
8.5.3 Configure Authentication Code 90
8.5.4 Select Tones 90
8.5.5 Set Default Language 90
8.5.6 Set Frequency Band 90
8.5.7 Enable Carriers 91
8.5.8 Local R-Key Handling 91
8.5.9 No Transfer on Hangup 91
8.5.10 Configure Coder 91
8.5.11 Secure RTP 92
8.5.12 Configure Supplementary Services 92
8.5.13 Select Mode 94
8.5.14 Set Master Id 94
8.5.15 Enable PARI Function 94
8.5.16 Configure Gatekeeper 95
8.5.17 Registration for Anonymous Devices 97
8.5.18 Select Mobility Master Mode 97
8.5.19 Connect Mobilty Master to other Mobility Master(s) 98
8.5.20 Disconnect Mobilty Master from other Mobility Master(s) 98
8.5.21 Connect Master to a Mobility Master 98
8.5.22 Enable the Radio 98
8.5.23 Enter IP Address to the PARI Master and the Standby PARI Master 99
8.5.24 Multiple Radio Configuration 99
8.5.25 PARI 99
8.5.26 SARI 100
8.5.27 Configure Air Synchronization 100
8.6 VoIP 102
8.6.1 Add instance id to the user registration with the IP-PBX 102
8.6.2 IP-PBX supports redirection of registration when registered to alternative proxy 102
8.6.3 Use local contact port as source port for TCP/TLS connections 102
8.6.4 Session Timer (initial value) 103
8.7 UNITE 103
8.7.1 Configure Messaging 103
8.7.2 Device Management 104
8.7.3 Service Discovery 104
8.7.4 Send Status Log 104
8.7.5 Module Fault List 105

8.8 Import and Export a Central Phonebook 105
8.9 Users 106
8.9.1 Show all Registered Users in the IP-DECT System 106
8.9.2 Search for User Information 106
8.9.3 Add a User 106
8.9.4 Import Users from a csv file 106
8.9.5 Export the Users to a csv file 107
8.9.6 Show Anonymous 107
8.10 Device Overview 107
8.10.1 Radios 107
8.10.2 RFPs 109
8.10.3 Sync Ring 109
8.10.4 Sync Ports 109
8.10.5 Air Sync 110
8.10.6 Sync Lost Counter in IPBS 110
8.11 DECT Sync 111
8.11.1 Air Sync Overview 111
8.11.2 Disturbances 113
8.11.3 Status 113
8.12 Traffic 113
8.12.1 Display All Ongoing Calls in the System 113
8.12.2 Display Calls 114
8.12.3 Handover 114
8.13 Gateway 114
8.13.1 General 114
8.13.2 Interfaces 115
8.13.3 SIP Interfaces 115
8.13.4 Gatekeeper Interfaces 119
8.13.5 Routes – Configuration 122
8.13.6 Show Active Calls 125
8.14 Backup 126
8.15 Software Upgrade 127
8.15.1 Before Upgrading 127
8.15.2 Upgrading Sequence 127
8.15.3 IPBS/IPBL Upgrade 128
8.15.4 Configuration After Updating the Firmware From Software Version 2.x.x to Later 128
8.15.5 Configuration After Updating the Firmware From Software Version 3.x.x to Later 129
8.15.6 System Upgrade from Software Version 4.x.x to 5.0.x 130
8.16 System Downgrade from software version 5.0.x to 2.x.x, from 4.x.x to 2.x.x and from 3.x.x to 2.x.x 130

8.17 System Downgrade from software version 5.0.x to 3.x.x and 4.x.x to 3.x.x ... 130
8.18 Update ... 130
8.18.1 Update Configuration ... 130
8.18.2 Update Firmware ... 131
8.18.3 Update the Boot File ... 131
8.18.4 Update the RFPs ... 131
8.19 System Upgrade in System with Mobility Masters ... 132
8.20 Replacing Master Hardware in Multiple Master System ... 133
8.21 Diagnostics ... 133
8.21.1 Logging ... 133
8.21.2 Tracing ... 134
8.21.3 Alarms ... 134
8.21.4 Events ... 135
8.21.5 Performance ... 136
8.21.6 Config Show ... 136
8.21.7 Ping ... 137
8.21.8 Traceroute ... 137
8.21.9 Environment ... 137
8.21.10 RFP Scan ... 137
8.21.11 Service Report ... 137
8.22 Reset ... 138
8.22.1 Idle Reset ... 138
8.22.2 Immediate Reset ... 138
8.22.3 TFTP Mode ... 138
8.22.4 Boot ... 138
8.23 Reset Using the Reset Button ... 138

9 Commissioning ... 140
9.1 Radio coverage verification tests ... 140
9.1.1 Base Station Operation Test ... 140
9.1.2 Coverage Area Test ... 140
9.1.3 Evaluation ... 140
9.2 Cordless Extension Number Test ... 140

10 Troubleshooting ... 142
10.1 Load Firmware Using the Gwload Tool ... 142
10.2 Fault Code Descriptions ... 142

11 Related Documents ... 146
Appendix A: How to Use the Update Server ... 148
Appendix B: RFP Power Consumption ... 153
Appendix C: Local R-Key Handling ... 155
Appendix D: Database Maintenance ... 156

Appendix E: Load Balancing 158
Appendix F: Update Script for Configuration of Kerberos Clients 165
Appendix G: Install Certificate in the Web Browser 166

1 Introduction

This document describes how to install and operate the following equipment:

- IPBS [1]
- IPBL [2]

The document is intended as a guide for installation, troubleshooting and maintenance purposes and are relevant for the following personnel:

- System administrator
- Service technician

For information on the IP-DECT system, see the applicable System Description documentation for IP-DECT.

For information about supported PBXs contact your supplier.

1.In previous documentation, *IPBS Base Station* (or *IPBS*) was sometimes referred to as *IP-DECT Base Station*.
2.IIn previous documentation, *IPBL* was sometimes referred to as *IP-DECT Gateway*.

1.1 Abbreviations and Glossary

Base Station	Common name for IPBS, DECT Base Station (BS3x0) and TDM-DECT Base Station.
DECT	Digital Enhanced Cordless Telecommunications: global standard for cordless telecommunication.
DECT Base Station	Another name for *BS3x0*
TDM-DECT Base Station	Another name for DB1.
DHCP	Dynamic Host Configuration Protocol
DTMF	Dual Tone Multiple-Frequency
FER	Frame Error Rate
GUI	Graphical User Interface
IP	Internet Protocol: global standard that defines how to send data from one computer to another through the Internet
IPBL	Previously called *IP-DECT Gateway* or, more commonly, as "the Blade"
IPBS	Also referred to as *IPBS Base Station*. Previously called *IP-DECT Base Station*
LAN	Local Area Network: a group of computers and associated devices that share a common communication line.
LDAP	Lightweight Directory Access Protocol
PBX	Private Branch Exchange: telephone system within an enterprise that switches calls between local lines and allows all users to share a certain number of external lines.
PSCN	Primary receiver Scan Carrier Number: defines the RF carrier on which one receiver will be listening on the next frame.
RFP	Radio Fixed Part. DECT base Station part of the DECT Infrastructure.
RFPI	Radio Fixed Part Identity
RSSI	Radio Signal Strength Information
RTP	Real-Time Transport Protocol
SST	Site Survey Tool
ToS	Type of Service
VLAN	Virtual Local Area Network

2 Description

This section gives a general description of the following devices:

- IPBS1, see *2.1 IPBS1*
- IPBS2, see 2.2 *IPBS2* on page 6
- IPBL, see 2.3 *IPBL* on page 10
- DECT Base Station, see 2.4 *DECT Base Station (BS3x0)* on page 13.
- TDM-DECT Base Station, see 2.5 *DB1* on page 15

2.1 IPBS1

The following versions of the IPBS1 are available:

- IPBS1 with internal antenna
- IPBS1 with external antennas

2.1.1 IPBS1 with Internal Antenna

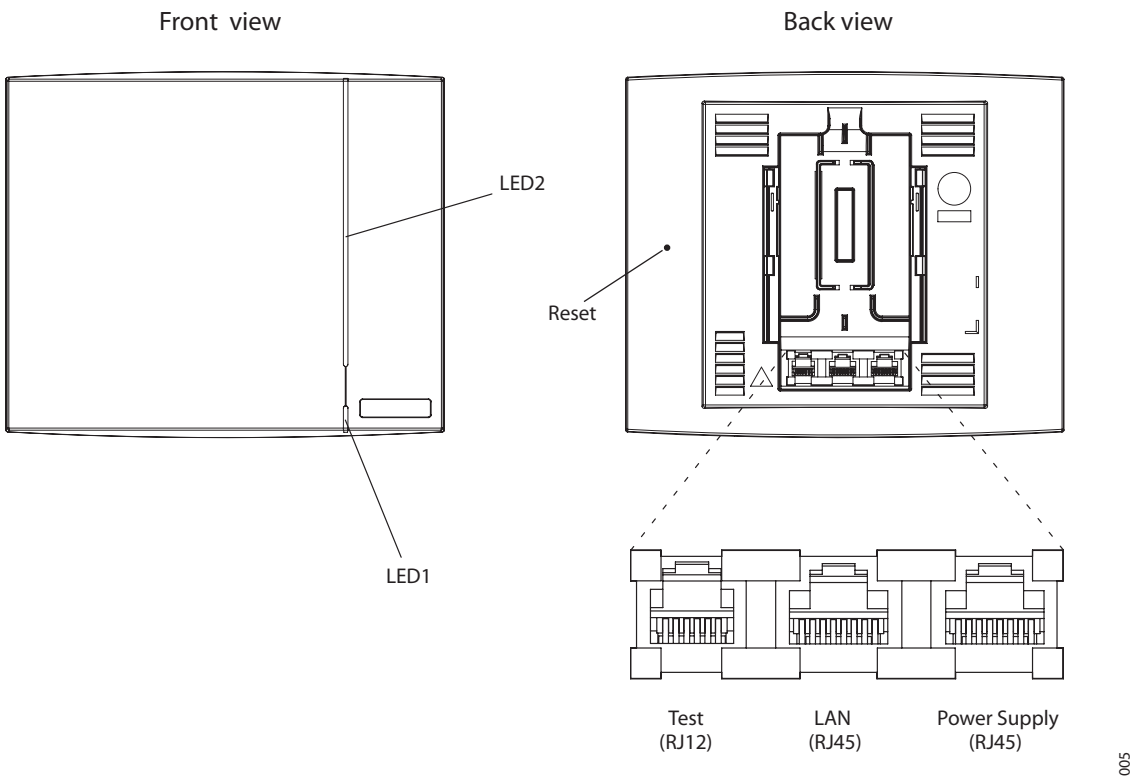


Figure 1. IPBS1 Overview

Contents of the Box

The box in which the IPBS1 is packed contains:

- An IPBS1 with integrated antennas
- A mounting bracket
- Two screws with wall plugs

Power Distribution

The IPBS1 can be powered using the following methods:

- Power over Ethernet, IEEE 802.3af
- A local AC-adapter

Note: For more information about power distribution, see 5.3 *Power the Base Station* on page 34.

Software

The software in the IPBS1 can be updated by downloading new software without disconnecting the equipment. The new software is stored in flash memory. See 8.18 *Update* on page 130 for information.

Connectors

- Two 8-pin RJ45 modular jacks for LAN/PoE and powering
- A 6-pin RJ12 modular jack for factory testing

LEDs

Status of LED1 (lower LED)	Description
Steady Green	Operational
Flashing fast amber	Download of firmware in progress.
Steady Amber	TFTP mode
Alternating red/green	No Ethernet connection

Status of LED2 (upper LED)	Description
Not lit	IPBS1 operational and no traffic on the IPBS1.
Steady green	IPBS1 operational and traffic on the IPBS1.
Flashing slow green	Fully occupied with traffic.
Flashing red	No air synchronization - searching for air sync candidates.
Flashing fast red	Download of RFP software in progress.
Alternating red/green	RFP not initialized.

2.1.2 IPBS1 with External Antennas

The IPBS1 is available with two omni-directional external antennas. Other external antennas can be mounted as well. This section contains the differences between the IPBS1 with internal and external antennas. For all other information see 2.1.1 *IPBS1 with Internal Antenna* on page 3.

Contents of the Box

The box in which the IPBS1 is packed contains:

- An IPBS1 for external antennas
- Two antennas
- A mounting bracket
- Two screws with wall plugs

Note: The IPBS1 cannot be mounted with the antennas pointing downwards as the mounting bracket does not support it.

Insert the antennas into the IPBS1 before following the installation instructions in 5.2 *Install the Base Station* on page 27.

2.2 IPBS2

The following versions of the IPBS2 are available:

- IPBS2 with internal antenna
- IPBS2 with external antennas

The IPBS2 is backward compatible with the IPBS1 when it comes to coverage, functionality, accessories and mounting bracket. If an old IPBS1 has to be replaced you just reuse the mounting bracket and install the IPBS2.

2.2.1 IPBS2 with Internal Antenna

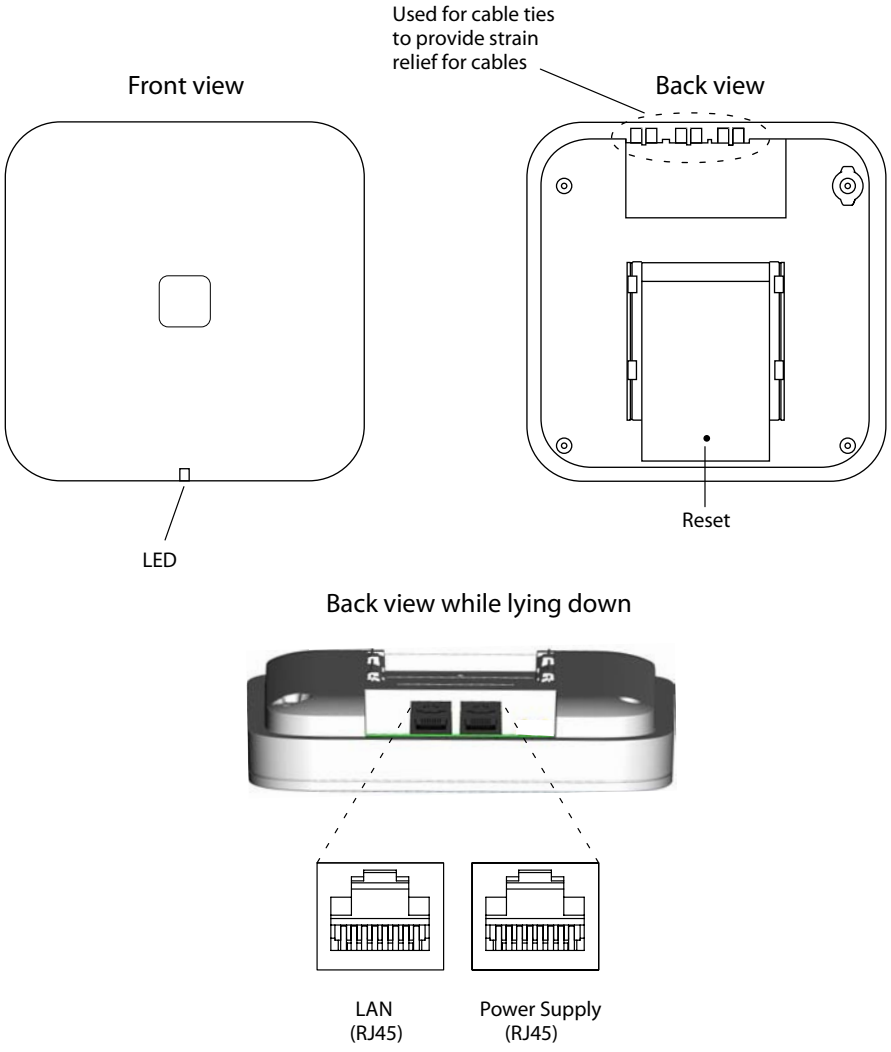


Figure 2. IPBS2 Overview

Contents of the Box

The box in which the IPBS2 is packed contains:

- An IPBS2 with integrated antennas
- A mounting bracket
- Two screws with wall plugs

Power Distribution

The IPBS2 can be powered using the following methods:

- Power over Ethernet, IEEE 802.3af
- A local AC-adapter

Note: For more information about power distribution, see 5.3 *Power the Base Station* on page 34.

Software

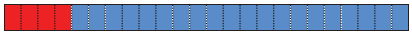
The software in the IPBS2 can be updated by downloading new software without disconnecting the equipment. The new software is stored in flash memory. See 8.18 *Update* on page 130 for information.

Connectors

- Two 8-pin RJ45 modular jacks for LAN/PoE and powering

LEDs

The IPBS2 has one RGB LED to indicate status. This section describes the different indications and when they shall be used. In the illustrations below: Each blink pattern is represented by a number of blocks where each block is 100 ms. Light grey blocks means that the LED is off. Whenever the indication is changed the new pattern always starts from the first block.

Idle/OK	Solid blue.	IPBS2 operational and no traffic on the IPBS2.
Starting up/ searching	100 ms blue, 100 ms off.	The IPBS2 is in start-up phase, e.g. waiting for parameters from PARI Master, or is searching for air synchronization.
Active traffic	400 ms off, 2000 ms blue.	IPBS2 operational and traffic on the IPBS2.
Fully occupied for speech traffic	400 ms red, 2000 ms blue. 	Fully occupied with traffic.
Software download	400 ms blue, 600 ms off.	Download of firmware in progress.
Mini firmware	100 ms yellow, 100 ms off.	The IPBS2 is in mini firmware mode.

TFTP mode	Solid yellow.	TFTP mode.
Error	100 ms red, 100 ms off.	No Ethernet connection.
Fatal error	Solid red.	Fatal hardware error.
Deployment: Good sync	2000 ms blue, 400 ms yellow.	The IPBS2 is in deployment mode and has good air sync coverage.
Deployment: Bad sync	400 ms blue, 600 ms off, 400 ms blue, 600 ms off, 400 ms yellow.	The IPBS2 is in deployment mode and does not have adequate air sync coverage.
Deployment: No sync	2000 ms red, 400 ms yellow.	The IPBS2 is in deployment mode and has no air sync coverage.

2.2.2 IPBS2 with External Antennas

This section contains the differences between the IPBS2 with internal antenna and the IPBS2 with external antennas. For all other information see 2.2.1 *IPBS2 with Internal Antenna* on page 6.

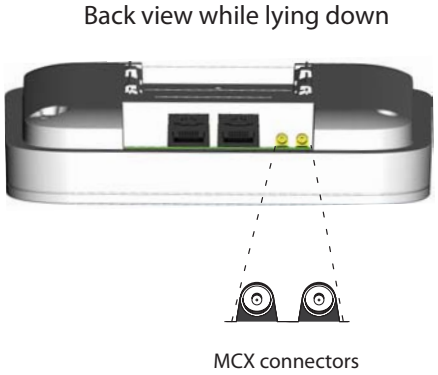


Figure 3. IPBS2 with MCX connectors for external antennas.

Contents of the Box

The box in which the IPBS2 is packed contains:

- An IPBS2 with external antennas.

- A mounting bracket
- An antenna bracket
- Two antenna coaxial cables.
- Two antennas.
- Four screws with wall plugs

2.3 IPBL

The following versions of the IPBL are available:

- IPBL IP-DECT Gateway VAC/VDC (for 110/230 VAC or 48 VDC)
- IPBL IP-DECT Gateway VDC (for 48 VDC)

2.3.1 Overview

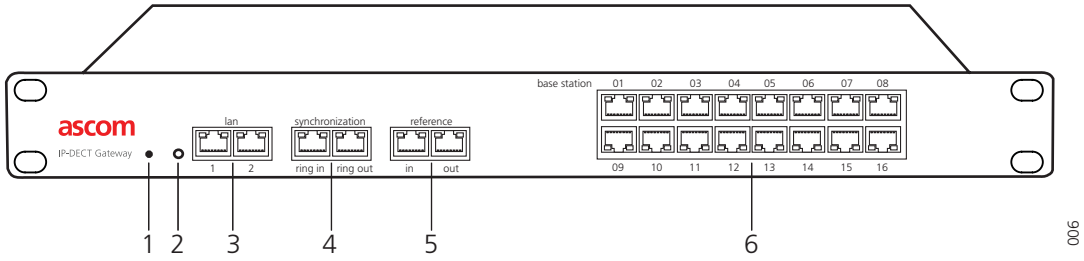


Figure 4. Overview of the IPBL

Pos.	Name	Function
1	Reset	Resets the IPBL, see 8.23 *Reset Using the Reset Button* on page 138 for more information.
2	Status LED	Indicates the status on the IPBL.
3	Lan	10BASE-T/100BASE-T Ethernet interface. LAN1 port must be used in the IP-DECT system (LAN2 port is for administration only).
4	Synchronization	Sync ring in and sync ring out interfaces.
5	Reference	Reference sync in and reference sync out interfaces.
6	Base station 01-16	ISDN U_{PN} DECT base station interfaces.

2.3.2 Power Supply

The power supply are located at the rear of the IPBL. The IPBL can be powered using the following alternatives:

- 110/230 VAC (*only IPBL IP-DECT Gateway VAC/VDC*)
- 48 VDC

Note: For more information, see 6.3 *Power the IPBL* on page 40.

Software

The software in the IPBL can be updated by downloading new software without disconnecting the equipment. The new software is stored in flash memory. See 8.18 *Update* on page 130 for information.

2.3.3 LED indication

Status LED	**Description**
Not lit	Not powered, status is not defined.
Flashing slow green	When pressing the reset button.
Flashing fast green	Firmware update or clear config after long reset.
Steady green	Status OK, system is fully operational.
Steady red	Status Fail, system error condition.
Steady amber	System is in TFTP server mode.

Base station LED	**Description**
Not lit	No U_{PN} link established.
Flashing	U_{PN} link established (activated state), RFP is not operational.
Steady	RFP is fully initialised and operational.

Base station LED	**Description**
Not lit	No speech activity in RFP.
Flashing	All speech channels occupied in RFP.
Steady	Speech activity in RFP.

Sync/Ref sync LED	**Description**
Not lit	No sync communication established.
Steady	Communication established.

Sync/Ref sync LED	**Description**
Not lit	Sync port not selected as input sync source.
Flashing	Sync port selected as input sync source but the sync signal is not in sync.
Steady	Sync port selected as input sync source and the sync signal is in sync.

Lan LED	**Description**
Not lit	No link.
Flashing	Link present and network activity.
Steady	Link present, but no network activity.

Lan LED	**Description**
Not lit	10 Mbps operation.
Steady	100 Mbps operation.

2.4 DECT Base Station (BS3x0)

The following versions are available:

- BS330 with Internal antenna
- BS340 with External antennas

2.4.1 DECT Base Station

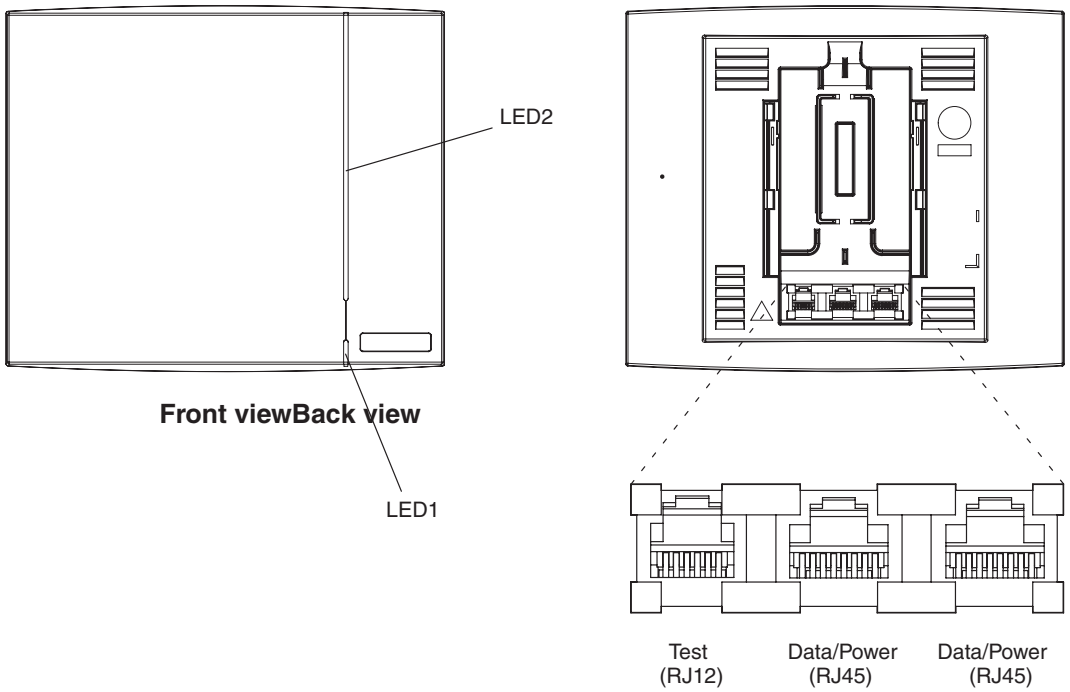


Figure 5. BS3x0 Overview

Contents of the Box

The box in which the base station is packed contains:

- A base station
- Two antennas (only base station with external antenna)
- A mounting bracket
- Two screws with wall plugs

Power Distribution

The base station can be powered using the following methods:

- From the IPBL via the Express Powering Pair (EPP) and data pairs
- With a local AC-adapter

Note: For more information about power distribution, see 5.3 *Power the Base Station* on page 34.

Software

The software in the BS3x0 can be updated by downloading new software without disconnecting the equipment. The new software is stored in flash memory. See 8.18 *Update* on page 130 for information.

Connectors

- Two 8-pin RJ45 modular jacks for data and powering
- A 6-pin RJ12 modular jack for factory testing

LEDs

Status of LED1 (lower LED)	Description
Steady Green	Power LED

Status of LED2 (upper LED)	Description
Not lit	Base station operational and no traffic on the base station.
Flashing green	Fully occupied with traffic.
Steady green	Base station operational and traffic on the base station.
Flashing amber	Software is being downloaded to the base station
Steady amber	Base station is OK, but not available (self-test, not initialized, no communication with IPBL)

2.5 DB1

The following versions of the DB1 are available:

- DB1 with internal antenna
- DB1 with external antennas

The DB1 is backward compatible with the BS3x0 when it comes to coverage, functionality, accessories and mounting bracket. If an old BS3x0 has to be replaced you just reuse the mounting bracket and install the DB1.

2.5.1 DB1 with Internal Antenna

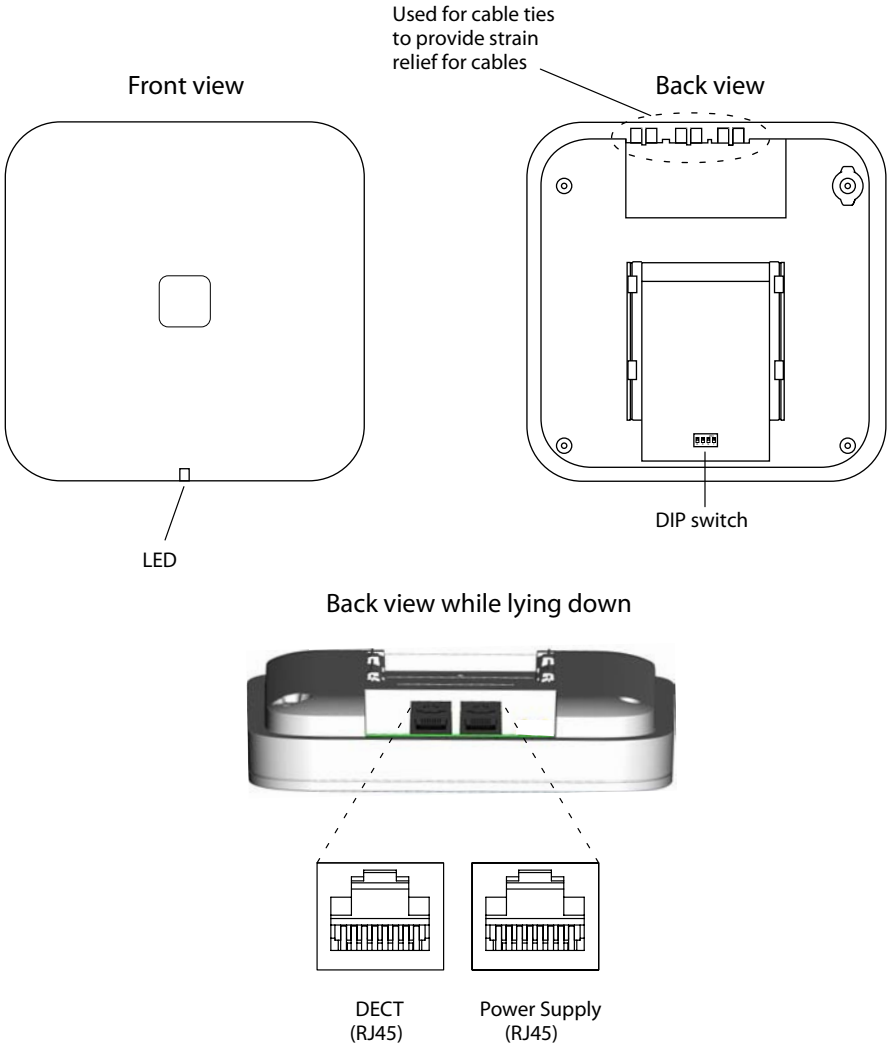


Figure 6. DB1 Overview

Contents of the Box

The box in which the DB1 is packed contains:

- A DB1 with integrated antennas
- A mounting bracket
- Two screws with wall plugs

Power Distribution

The DB1 can be powered using the following methods:

- From the IPBL via the Express Powering Pair (EPP) and data pairs
- With a local AC-adapter

Note: For more information about power distribution, see 5.3 *Power the Base Station* on page 34.

Software

The software in the DB1 can be updated by downloading new software without disconnecting the equipment. The new software is stored in flash memory. See 8.18 *Update* on page 130 for information.

Connectors

- Two 8-pin RJ45 modular jacks for data and powering

LEDs

The IPBS2 has one RGB LED to indicate status. This section describes the different indications and when they shall be used. In the illustrations below: Each blink pattern is represented by a number of blocks where each block is 100 ms. Light grey blocks means that the LED is off. Whenever the indication is changed the new pattern always starts from the first block.

Idle/OK	Solid blue.	DB1 operational and no traffic on the DB1.
Starting up	100 ms blue, 100 ms off.	The DB1 is in start-up phase, i.e. waiting to be initialized by the IPBL.
Active traffic	400 ms off, 2000 ms blue.	DB1 operational and traffic on the DB1.
Fully occupied for speech traffic	400 ms red, 2000 ms blue.	Fully occupied with traffic.
Software download	400 ms blue, 600 ms off.	Download of firmware in progress.
Error	100 ms red, 100 ms off.	U_{PN} layer 1 communication error.

Fatal error	Solid red.	Fatal hardware error.

DIP Switches

The DIP switches can be found on the back of the DB1, see figure 6 on page 15.

Note: DIP switch 3 and 4 shall be set to ON.

Set DIP switch 1 and 2 to ON or OFF as follows:

DIP switch 1: ON DIP switch 2: ON	Europe frequency
DIP switch 1: OFF DIP switch 2: ON	China frequency
DIP switch 1: ON DIP switch 2: OFF	South America frequency
DIP switch 1: OFF DIP switch 2: OFF	North America frequency

2.5.2 DB1 with External Antennas

This section contains the differences between the DB1 with internal antenna and the DB1 with external antennas. For all other information see 2.5.1 *DB1 with Internal Antenna* on page 15.

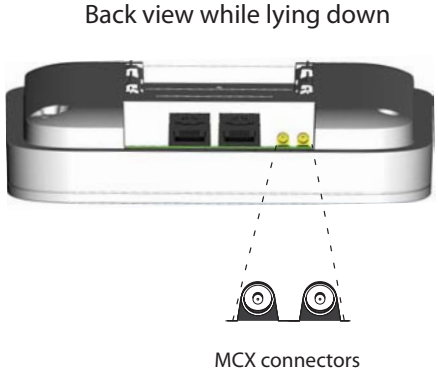


Figure 7. DB1 with MCX connectors for external antennas.

Contents of the Box

The box in which the DB1 is packed contains:

- A DB1 with external antennas.
- A mounting bracket
- An antenna bracket
- Two antenna coaxial cables.
- Two antennas.
- Four screws with wall plugs

2.6 AC-adapter

The AC-adapter is used to power a base station locally.

Note: The maximum length of cable from adapter must not exceed 10 meters.

Versions (different type of mains plug)

For European countries except U.K.	Art. no.: 130137B	Order. no.: BSX-0013
For U.K.	Art. no.: 130136B	Order. no.: BSX-0014
For NA	Art. no.: 130138A	Order. no.: BSX-0015
For Australia	Art. no.: 130139B	Order. no.: 660263

IMPORTANT: If local power supply is used for the RFPs, the EPP cable pair must NOT be connected.

3 Safety Instructions

For safe and efficient operation, observe the guidelines given in this manual and all necessary safety precautions. Follow the operating instructions and adhere to all warnings and safety precautions located on the product and this manual.

- Installation and service is to be performed by service persons only.
- IPBL must be connected to a mains socket outlet with a protective earthing connection.
- IPBL must be permanently connected to protective earth when powered by 48 VDC.
- IPBL must be mounted in a Restricted Area Location (RAL) in Sweden, Finland and Norway.
- Ensure that the voltage and frequency of the mains power socket matches the voltage and frequency inscribed on the equipment's electrical rating label.
- Never install telephone wiring during a thunderstorm.

Note: Avoid touching or punching down the IPBS/RFP signal and power pairs as there is 48Vdc or 24Vdc present on these wires at all times.

- Always install the base station conforming to relevant national installation rules.
- Disconnect all power sources before servicing the equipment.
- Use only approved spare parts and accessories. The operation of non-approved parts cannot be guaranteed and may cause damage or danger.
- Only approved power supplies according to valid editions of EN/IEC/CSA/UL/AU/NZS 60950 are to be used when the IPBS/RFPs are powered by local power supplies.

3.1 Protection Against Electrostatic Discharge (ESD)

Integrated circuits are sensitive to ESD.To avoid damage caused by ESD, service engineers and other people must handle equipment and boards carefully.

Electronic equipment has become more resistive to ESD, but we see an increase of situations where static electricity can build up. This is caused by an increasing application of man–made fibres like nylon, acrylic, etc. which are capable of generating ESD of 10,000 Volts and more.

Walking across a nylon carpet, even for a few feet, could cause a person to be charged–up to more than 10,000 Volts.
Under these conditions, if a system board or a (C)MOS device is touched it could easily be damaged. Although the device may not be totally defective, it is often degraded, causing it to fail at a later date without apparent reason.

To make sure that equipment and parts are well protected during shipment, special packaging materials are utilized. System boards will be shipped in anti–static bags and (C)MOS devices and other sensitive parts in small shielded boxes.

3.1.1 ESD Handling

In the interest of quality and reliability, it is advisable to observe the following rules when handling system parts:

- Keep parts in their protective packaging until they are needed.
- When returning system parts like EEPROMS to the factory, use the protective packaging as described.
- Never underestimate the damaging power ESD can have and be especially careful when temperatures are below freezing point and during very warm weather in

combination with low humidity. Make sure that the environmental conditions remain within the limits specified in the components' data sheets.

IMPORTANT: In the interest of quality and reliability system boards and other parts returned for exchange or credit may be refused if the proper protective packaging is omitted!

3.2 Safety Aspects

3.2.1 IP-DECT Base Station

The IP-DECT Base Station meets the valid editions of safety standard EN/IEC/CSA/UL/AU/NZS 60950-1. The system is a class III equipment for stationary wall mounting.

3.2.2 DECT Base Station BS3x0 and TDM-DECT Base Station DB1

The DECT Base Station BS3x0 meets the valid editions of safety standard EN/IEC/CSA/UL/AU/NZS 60950-1. The system is a class III equipment for stationary wall mounting.

3.2.3 IP-DECT Gateway (IPBL)

The IPBL meets the valid editions of safety standard EN/IEC/CSA/UL/AU/NZS 60950-1.

3.3 Regulatory Compliance Statements (EU/EFTA only)

The equipment are intended to be used in the whole EU&EFTA.

The equipment are in compliance with the essential requirements and other relevant provisions of R&TTE Directive 1999/5/EC. The Declarations of Conformity may be consulted at:

http://www.ascom.com/ws/products_ws.htm

The IP-DECT Base Stations, BS3x0 Base Station, TDM-DECT Base Station DB1 and IP-DECT Gateway are marked with the label CE.

3.4 Regulatory Compliance Statements (USA and Canada only)

FCC compliance statements

The equipment have been tested and found to comply with the limits for a Class B digital device (Base Stations), pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. The equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and the receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/tv technician for help.

Information to user

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1 this device may not cause harmful interference, and

2 this device must accept any interference received, including interference that may cause undesired operation.

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

1 this device may not cause interference, and

2 this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

1 l'appareil ne doit pas produire de brouillage, et

2 l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

IC Requirements for Canada

This Class B digital apparatus (Base Stations) complies with Canadian ICES-003.

Cet appareil numérique (stations de base) de la Classe B conforme á la norme NMB-003 du Canada.

This Class A digital apparatus (IP-DECT Gateway) complies with Canadian ICES-003.

Cet appareil numérique (IP-DECT Gateway) de la Classe A conforme á la norme NMB-003 du Canada.

Modifications

Any modifications not expressly approved by Ascom could void the user's authority to operate the equipment.

Exposure to radio frequency signals

This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. The antenna used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

4 IP Security

4.1 IP Security Terminology

4.1.1 SSL/TLS

Note: Secure Socket Layer (SSL) has been renamed Transport Layer Security (TLS). TLS 1.0 is based on SSL 3.0/3.1. This document hereafter uses the term TLS.

TLS is a security mechanism based on cryptography (see *4.1.3 Cryptography*) and is used for encrypting communications between users and TLS-based Websites. The encryption prevents eavesdropping and tampering with any transmitted data.

TLS operates on the OSI Model Level 5 and uses PKI (see *4.1.2 Public Key Infrastructure*).

4.1.2 Public Key Infrastructure

Public Key Infrastructure (PKI) is a component of Public Key Cryptography (PKC) that uses:

- Public Key Certificates, see *Public Key Certificates (Digital Certificates)*
- Certificate Authorities, see *Certificate Authorities*

Public Key Certificates (Digital Certificates)

Public Key Certificates are used for key exchange and authentication. They are simply electronic documents (files) that incorporate a digital *signature* to bind together a *public key* with an *identity* (information such as the name or a person or organization, their address, and so forth).

The signature may be signed by a trusted entity called a Certificate Authority (CA), see *Certificate Authorities*.

The most common use of public key certificates is for TLS certificates (https websites).

Certificate Authorities

A Certificate Authority or Certification Authority (CA) is a trusted entity which issues public key certificates. The certificates contain a public key and the identity of the owner. The CA asserts that the public key belongs to the owner, so that users and relying parties can trust the information in the certificate.

Certificate Signing Request (CSR) or **Certification Request** is a message that is generated and sent to a CA in order to apply for a TLS certificate. Before the CSR is created a key pair is generated, the private key kept secret. The CSR will contain the corresponding public key and information identifying the applicant (such as distinguished name). The private key is not part of the CSR but is used to digitally sign the entire request. Other credentials may accompany the CSR.

If the request is successful, the CA will send back an identity certificate that has been digitally signed with the CA's private key.

A CSR is valid for the server where the certificate will be installed.

4.1.3 Cryptography

Cryptography is the encoding of messages to render them unreadable by anyone other than their intended recipient(s). Modern cryptography uses complex algorithms implemented on modern computer systems.

Cryptography tasks can be divided into the two general categories Encryption and Authentication.

Encryption

Encryption is the scrambling of information so that the original message cannot be determined by unauthorized recipients by applying an *encryption algoritm* to the message *plaintext* producing *ciphertext* (appearently random bits). A *decryption algoritm*, if given the correct key, converts the ciphertext back into plaintext. Public key algoritms use paired keys, one for encryption and another for decryption.

Authentication

Authentication is the verification of a message's sender. This requires the message to be protected so it cannot be altered, usually by generating a *digital signature* formed by a hash of the message. Only the correct key can generate a valid signature.

4.2 Introduction to IP Security in IP-DECT

A secure system requires more planning than an unsecured system.

4.2.1 Secure Web Access (https)

For IP-DECT devices

- https access should be enabled
- http access should preferably be disabled

For more information see 8.1.7 *Configure the HTTP settings* on page 71 .

4.2.2 TLS Certificates

Security in Web-based applications rely on cryptography. Cryptographical systems are only as secure as their *keys.* This makes *Key Management* a critical and often neglected concern. *TLS Certificates* have emerged as a clever way of managing large scale key distribution.

Two certificate management tasks are needed for TLS:

3 Trust relationships when the device must know which third parties (e.g. IP-PBX) it shall trust in, see *1. Trust Relationships*.

4 Device certificates to authenticate the device against third parties, see *2. Certificate Handling Options with Device Certificates*.

1. Trust Relationships

Trust relationships are defined by a trust list in the device. The list contains the certificates to be accepted by the device for TLS secured connections (e.g. HTTPS, SIPS).

For more information see *Trust List* on page 74.

2. Certificate Handling Options with Device Certificates

There are three certificate handling options:

- Default Device certificate
  The default certificate is supplied with the device. It is a self-signed certificate. Self-signed certificates provide only encryption, not authentication.

  For more information see *Default Device Certificate* on page 76.

- Self-signed certificates
  This option is for customers not planning on having their certificates signed by public or private CAs. Self-signed certificates provide encryption but do in most cases not provide authentication.

  For more information see *Self-signed Certificates* on page 76.

- Certificates signed by a Certificate Authority (CA).
  Two options are possible:
  - **A)** Certificates signed by the customer's own CA. Customers possessing the knowledge and infrastructure to house their own CA could build an internal

enterprise CA, enabling them to sign (approve) their own certificate requests. This would make the customer a private CA.

- **B)** Certificates signed by a trusted public third party entity/organization. There are only about a dozen issuers who have the authority to sign certificates for servers worldwide. An example is VeriSign. To use a public CA for certificate approvals the IP-DECT system would in most cases need to be connected to the Internet and hold a fully qualified domain name. For more information see *Certificate Signing Request (CSR)* on page 77.

4.3 IP-DECT Administrative Functions

4.3.1 Configuration - HTTP

The HTTP tab is used to configure the type of web access that should be allowed for the device, includes a field for configuring https access.

For more information see 8.1.7 *Configure the HTTP settings* on page 71.

4.3.2 Configuration - Certificates

The *Certificates* tab lists the certificate used by web browsers to authenticate the identity of the device (Web server).

For more information see 8.1.10 *Certificates* on page 73.

4.3.3 Configuration - SIPS

SIP Secure (SIPS) is used to encrypt the signalling communication between the IPBS and the IP-PBX. SIPS uses the TLS protocol for encryption. The signalling between the IPBSs is also encrypted by default and there is no possibility to disable it.

For more information see 8.5.16 *Configure Gatekeeper* on page 95.

4.3.4 Configuration - Secure RTP

Secure RTP (SRTP) is used to encrypt the voice communication between the end user equipments. SRTP can be used with the Ascom VoIP Gateway.

For more information see 8.5.11 *Secure RTP* on page 92.

5 Installation of the Base Station

This section describes how to install the IPBSs, BS3x0 and DB1. Both base stations can be fixed to a wall, a ceiling, a pole or a beam, by means of the mounting bracket included. When fixing the base station to a wall or ceiling the included plugs and screws must be used. When fixing it to a pole or beam a strap or a flexible metal band must be used, this is not included.

Note: Fixing the base station to metal surfaces requires special consideration and is not recommended for several reasons. If this is unavoidable try to ensure a distance between the base station and the metal surface of, preferably, 1 meter.

5.1 Base Station Cabling

Recommended base station cable is a standard CAT5 unshielded ethernet cable with minimum 26 AWG copper conductors, this cable is also used for powering the base station. It is assumed that installation personnel know how to crimp RJ45 connectors to a cable.

Note: Since the distance between the base station and the wall is limited, a RJ45 modular jack without cable retention must be used.

Note: Ensure that during the installation of an base station, each base station is given an extra length (5-10 metres) of cable because it is possible that it will have to be moved for one reason or another.

5.2 Install the Base Station

The base station can be mounted vertically or horizontally. Mount the base station at places and positions as determined in the base station plan, see the applicable System Planning documentation for IP-DECT. The base station must be placed in a way that it is not facing large metal objects such as large heating pipes.

5.2.1 Fix the Mounting Bracket to a Wall

Fix the mounting bracket (see figure 8 on page 28) to the wall as follows:

1 Hold the mounting bracket with its flat side against the wall with the text 'TOP' upwards and mark the two holes. The minimum distance between the upper hole and the ceiling or any object above the base station must be at least 65 mm for IPBS1 and 100 mm for IPBS2 and DB1, see figure 8 on page 28. If the distance is less than 65/100 mm, the base station cannot be slid onto the bracket.

2 When using wall plugs: Drill the two holes using a ∅ 6 mm drill and insert the included wall plugs.

3 Position the mounting bracket with its flat side to the wall and fasten it with the two included ∅ 3.5 mm screws.

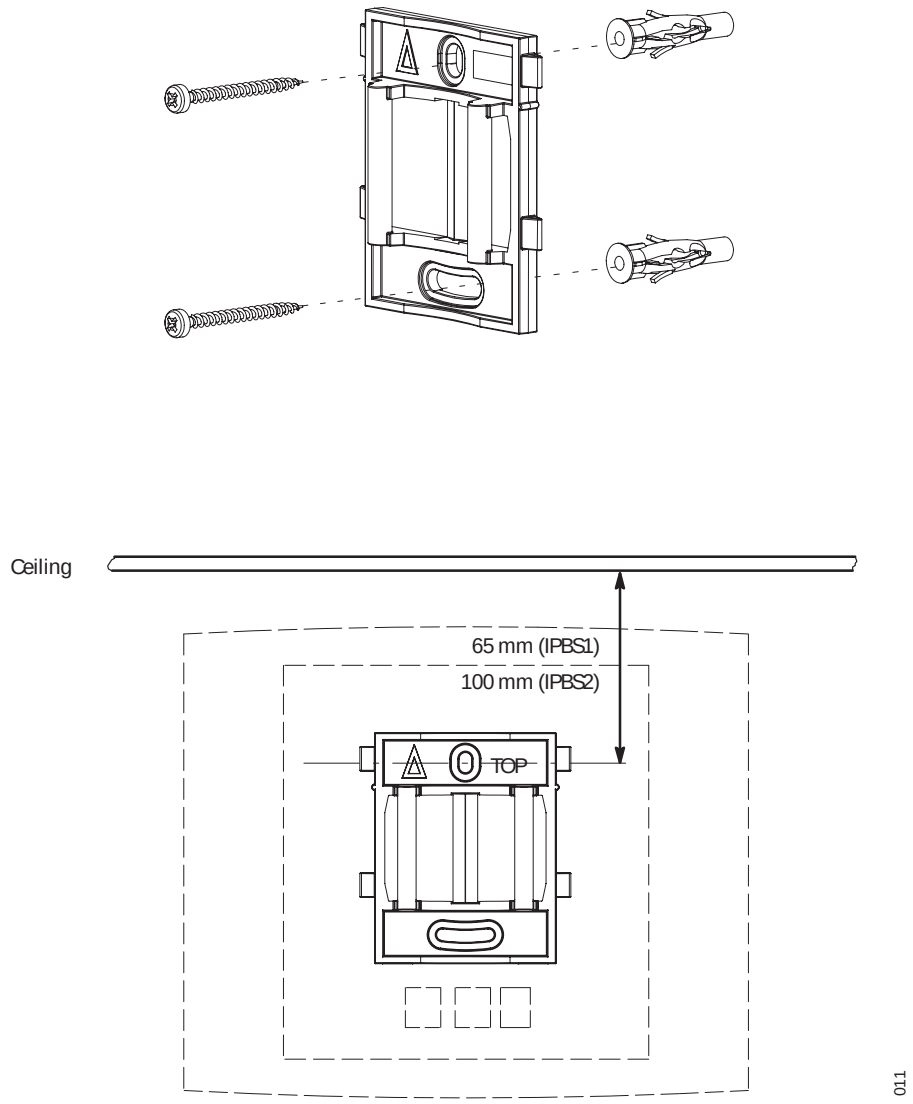


Figure 8. Fixing the mounting bracket to a wall.

5.2.2 Fix the Mounting Bracket to a Ceiling

Fixing to a ceiling is done in the same way as the a wall, see *5.2.1 Fix the Mounting Bracket to a Wall*. When the base station has to be positioned above a suspended ceiling, make sure that the front of the base station points downwards.

5.2.3 Fix the Mounting Bracket to a Pole or Beam

The mounting bracket can be fixed to a pole (diameter ≥ 45 mm) or a beam (wider than 50 mm) by means of a strap or flexible metal band less than 30 mm wide. The strap or flexible metal band is not included in the box.

1 Fix the mounting bracket to a pole or beam using the metal band, see figure 7 on page 29.

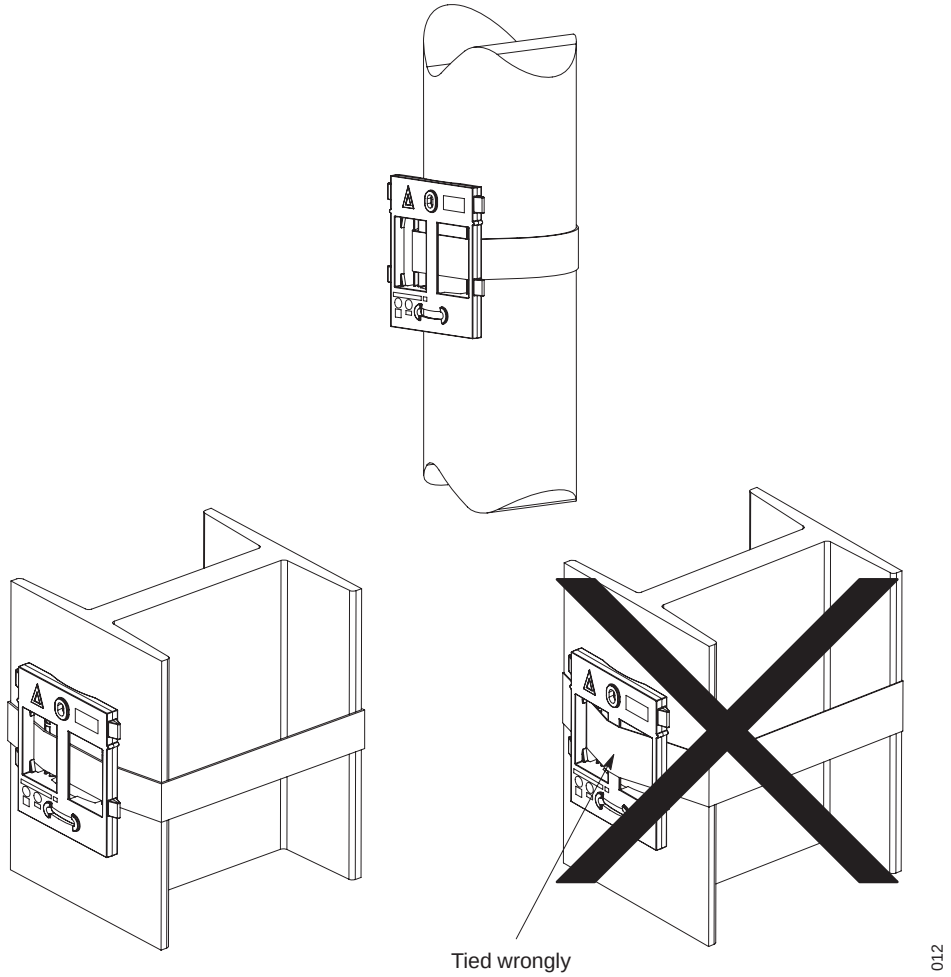


Figure 9. Fixing the mounting bracket to a pole or beam.

5.2.4 Use the Cable Ducts for IPBS1

When the base station IPBS1 is mounted to the wall, cable ducts can be used to route the wiring through.

1 Fix the cable duct to the wall in one of the positions shown in figure 8 on page 30.

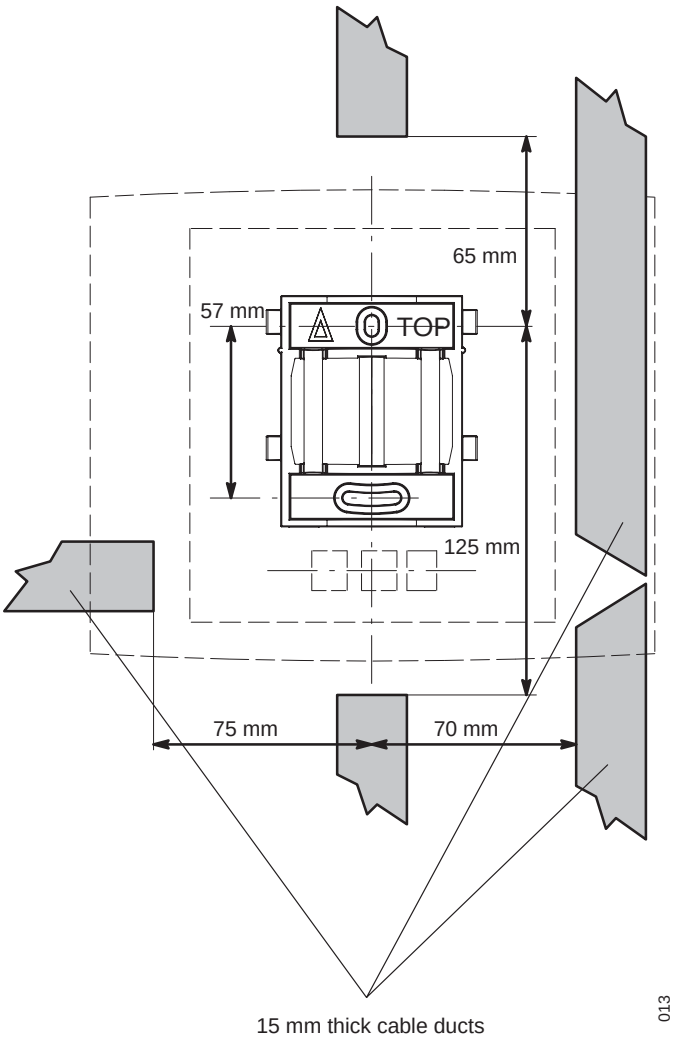
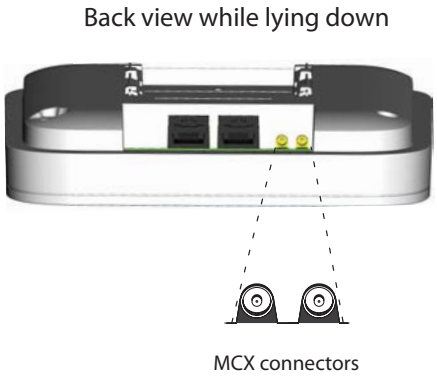


Figure 10. Minimum distances between a cable duct and the mounting bracket

5.2.5 Connect External Antennas (only IPBS2 and DB1)

1. Position the included antenna bracket above the mounting bracket with a minimum distance of 74 mm (250 mm maximum) and mark the two holes for the antenna bracket, see figure 11 on page 31 (1).
2. When using wall plugs: Drill the two holes using a ∅ 6 mm drill and insert the included wall plugs.
3. Position the antenna bracket to the wall and fasten it with the two included ∅ 3.5 mm screws.
4. Mount the two included coaxial cables on the antenna bracket figure 11 on page 31 (2). Fasten the coaxial cables with the lock nuts which are found on the coaxial cable antenna connectors.
5. Mount the antennas on the antenna connectors (2).

6 Connect the coaxial cables to the MCX connectors on the base station.



7 Mount the base station (3), see 5.2.9 *Mount the Base Station* on page 33.

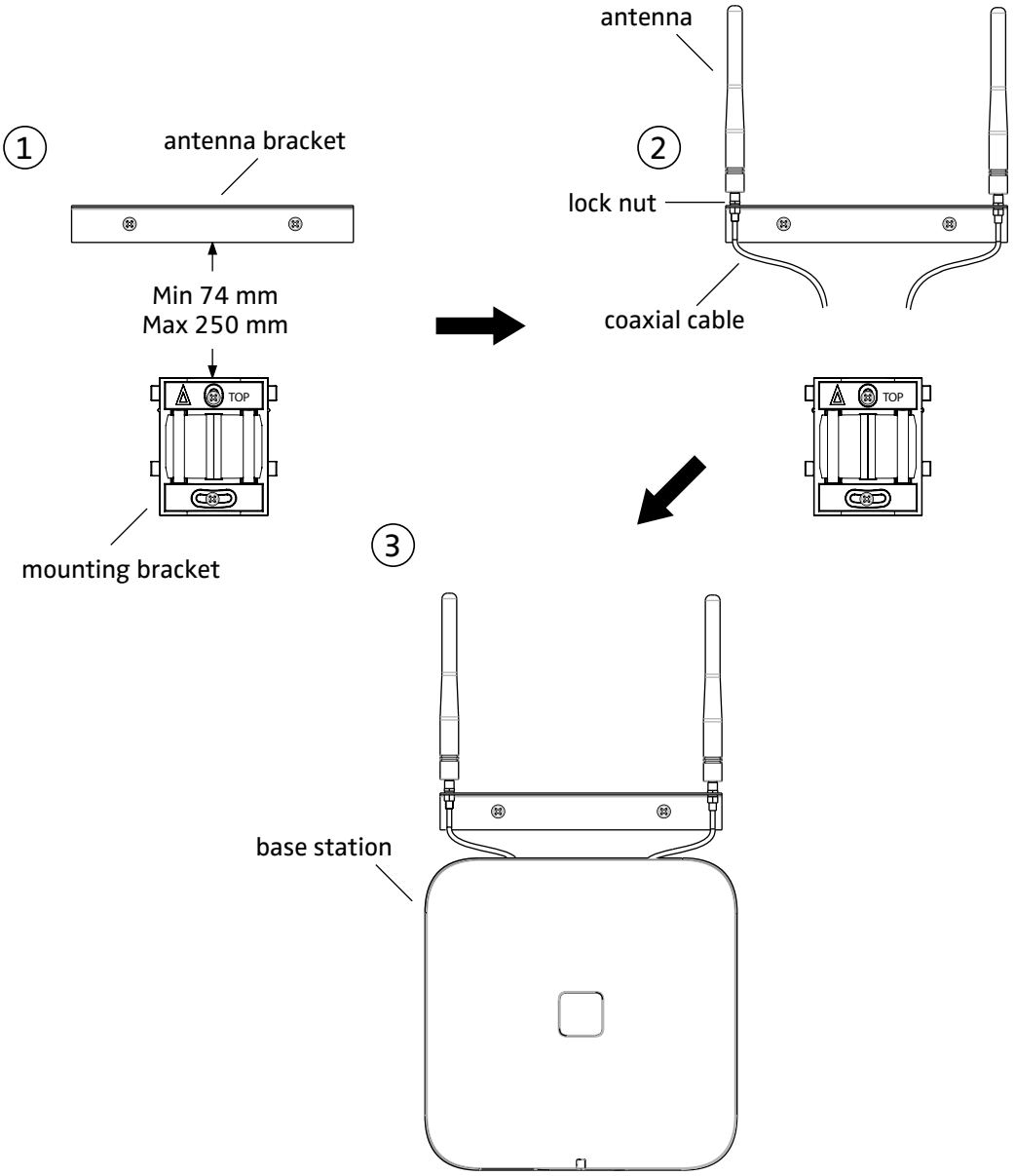


Figure 11. Connect external antennas.

5.2.6 Secure the Cable

For safety reasons secure the base station cable to a convenient point at about 30 cm from the base station.

If for some reason the base station drops, it is secured by the cable.

5.2.7 Pinning

1 Cut the cable to the correct length and connect the cable to a RJ45 modular jack.

2 For information on the pinning of the data jack see the following:

- IPBS, *Pin the IPBS Cable* on page 32.
- BS3x0 and DB1, *Pin the BS3x0/DB1 Cable* on page 33.

Do **not** plug the connector in the base station yet!

Note: Since the distance between the base station and the wall is limited, a RJ45 modular jack without cable retention must be used.

Pin the IPBS Cable

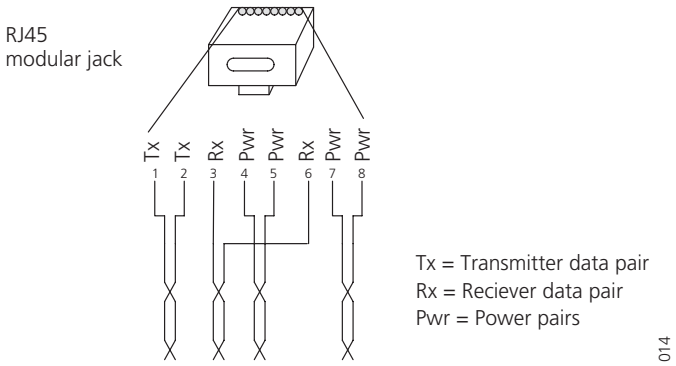


Figure 12. Connector pinning of the LAN/PoE connector, power feed over the spare cable pairs.

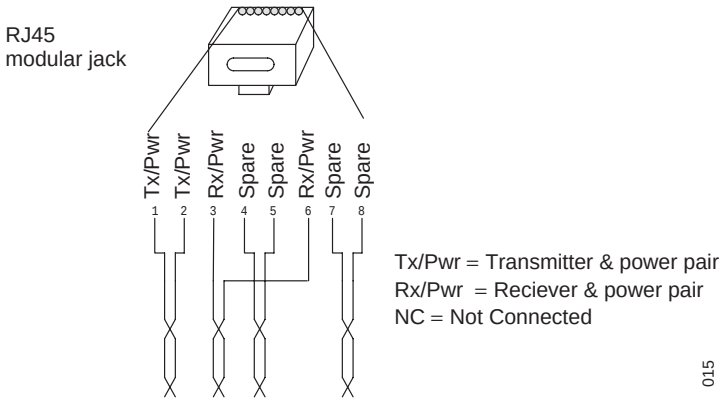


Figure 13. Connector pinning of the LAN/PoE connector, power feed over the Rx/Tx data cable pairs.

Pin the BS3x0/DB1 Cable

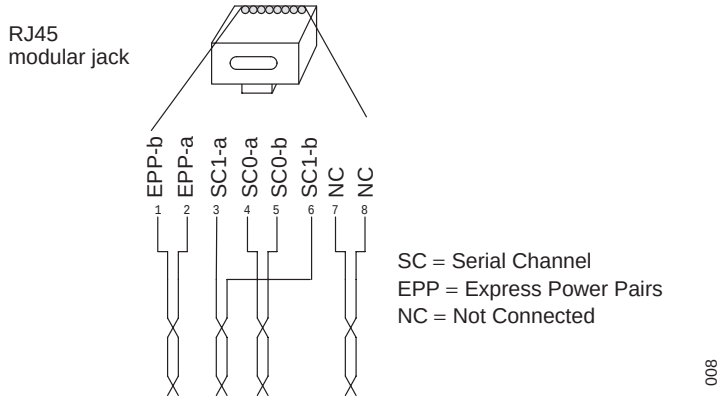
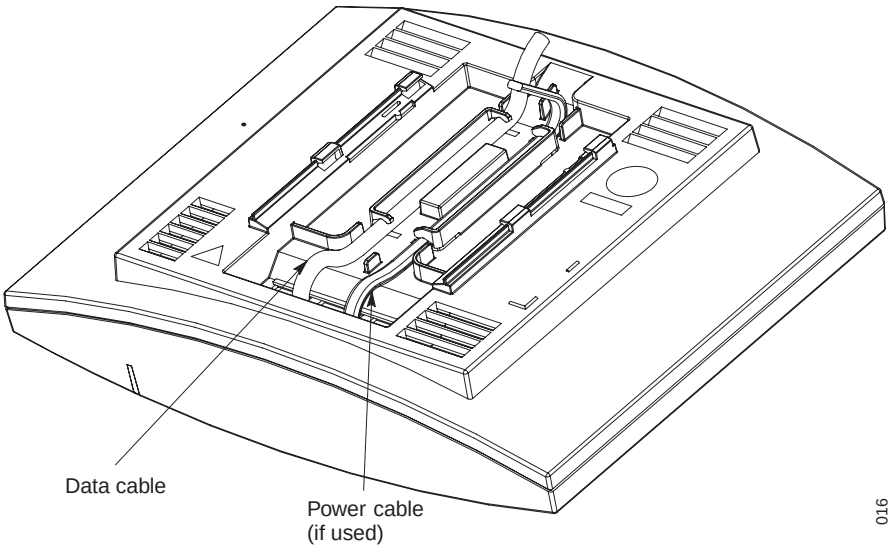


Figure 14. Connector pinning of the Data connector

IMPORTANT: If local power supply is used, the EPP cable pair must NOT be connected.

5.2.8 Connect the Base Station Cables

1 Only for IPBS1: If it is required that the cables enter the base station centrally from above, guide the cables through the recess in the middle of the base station as shown below.



2 Plug the modular jack of the data cable into one of the data/power connectors.

3 When an AC-adapter is used:

- Plug the modular jack of the AC-adapter in one of the data/power connectors.
- Plug the AC-adapter into a wall-outlet.

5.2.9 Mount the Base Station

Hold the base station flat against the mounting bracket and move it downwards until it clicks, see below.

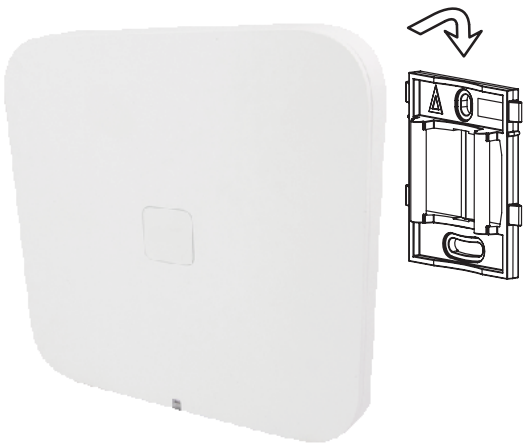


Figure 15. Mounting of the IPBS.

5.3 Power the Base Station

The base station is powered the following ways:

- Power over Ethernet (only IPBS).
- Power over Express Powering Pairs (EPP) and data pairs (only BS3x0 and DB1)
- By a local power supply.

Note: Do not power the base station using both power supplies. Parallel powering will not harm the base station but it can disturb the signalling.

5.3.1 Power the IPBS over Ethernet

The IPBS supports Power over Ethernet, IEEE 802.3af, class 2. The power source will allocate 7W to the IPBS. This must be regarded when planning the powering of the IPBSs so that the power limit of the PoE power source is not exceeded.

The PoE standard supports two ways of feeding the power:

1 Power over the Rx/Tx data pairs.

2 Power over the spare cable pairs.

Both power feed methods are supported in the IPBS, it is also insensitive to change of the polarity.

5.3.2 Power the BS3x0 and DB1 over Express Powering Pair (EPP) and data pairs

When a base station is powered remotely via the IPBL, the maximum length between the base station and the IPBL depends on the supply voltage, the number of twisted pairs used and the wire size. The length of the cable should never exceed "data-limited" length of the cable, see Appendix B: *RFP Power Consumption* on page 153.

5.3.3 Power the Base Station with a Local Power Supply

Powering the base station with a local power supply can be done using the second data/power inlet on the base station. The base station can be powered individually by an AC-adapter. The AC-adapter is provided with an 8-pin RJ45 plug that can be plugged into the *Power Supply* jack. For specification see 2.6 *AC-adapter* on page 18.

Note: Only approved power supply according to valid editions of EN/IEC/CSA/UL/AU/NZS 60950 is to be used when the base station is powered by a local power supply.

6 Installation of the IPBL

This section describes how to install the IPBL.

6.1 Install the IPBL

IMPORTANT: To keep the same functionality of the system, do not mix different RFPs, Core (KRCNB 201) with Worf (KRCNB 30x and BS3x0), on the same IPBL. The reason this will not work is prolonged preamle is supported by Worf RFPs but not by Core RFPs. When the handset receive capacity information from the RFPs, including prolonged preamble and multicast, it assumes that all RFPs are of the same type as the first RFP it receives data from.

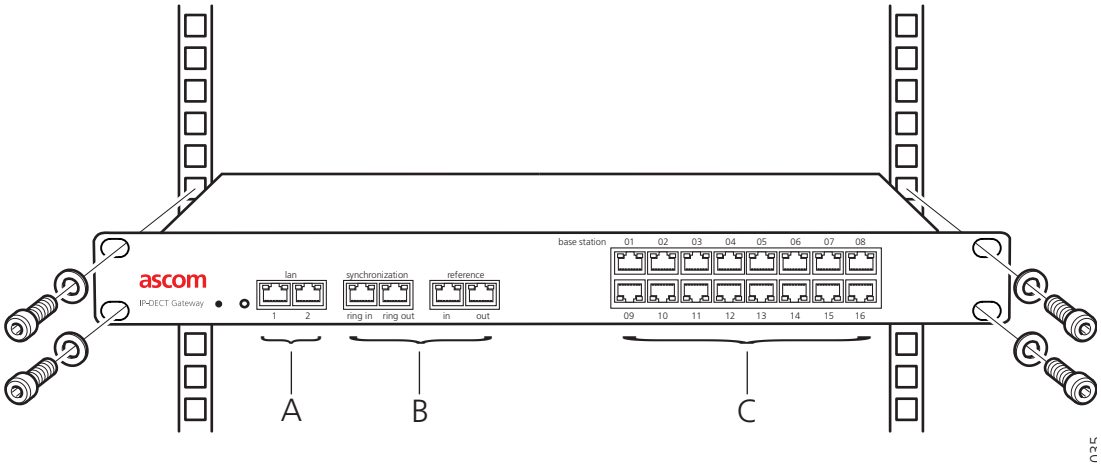


Figure 16. Install the IPBL

The main steps of the installation is described below:

1 Install the IPBL in a standard 19" rack.

2 Pin the cables, see 6.2 *Pin the IPBL Cable* on page 38.

3 Attach the power cable, see 6.3 *Power the IPBL* on page 40.

4 Connect the cables in the following order:

- Ethernet cable (A) LAN1 port must be used in the IP-DECT system (LAN2 port is for administration only).
- Synchronization cable (ring sync, reference sync) (B)
- Base station cable (RFP cable) (C)

IMPORTANT: The connected RFPs must not be connected to protective earth.

5 Monitor the total current consumption from the GUI. See 8.21.9 *Environment* on page 137. Make sure it not exceeds the following values:

- Max current consumption is 1,9/0,9 A when supplied with 110/230 VAC.
- Max current consumption is 5,2 A when supplied with 48 VDC.

Note: The IPBL current consumption is 0,3 A and is included in max current

consumption.

For more information of power consumption of the RFPs, see Appendix B: *RFP Power Consumption* on page 153.

6.2 Pin the IPBL Cable

All data cables used for the IPBL is standard CAT5 unshielded cable. It is assumed that installation personnel know how to crimp these connectors to a cable.

6.2.1 Synchronization Cable

The maximum cable length between two IPBLs must not exceed 2000 meters.

1 Cut the cable to the correct length.

2 Connect the cable to a RJ45 modular jack. For information on pinning, see Figure 13 and Figure 14.

3 Label the cable.

Sync IN

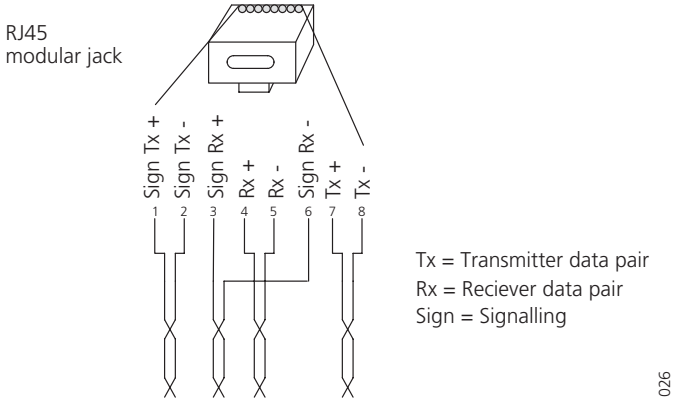


Figure 17. Connector pinning of the Sync IN cable

Sync OUT

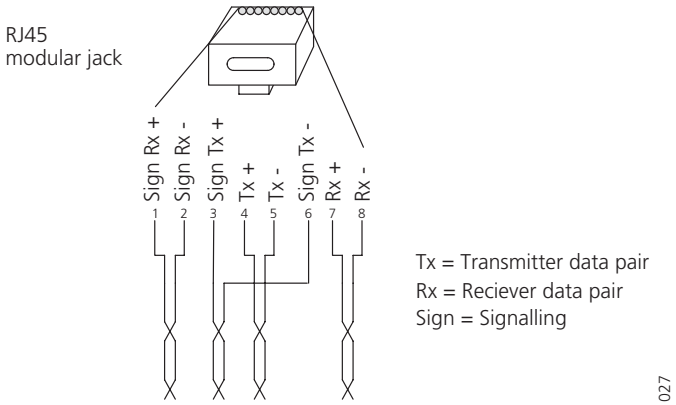


Figure 18. Connector pinning of the Sync OUT cable

6.2.2 RFP Cable

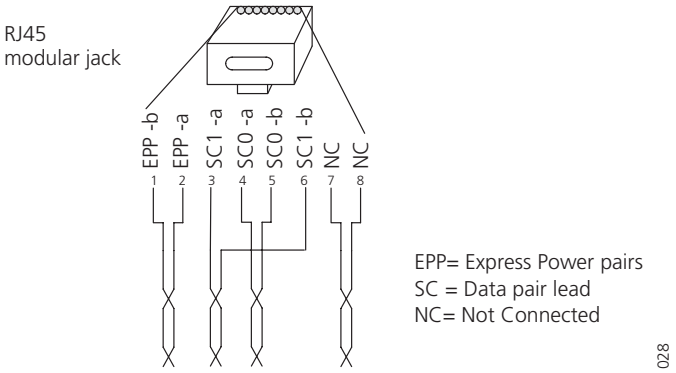
The RFP cable connects the IPBL with the RFPs. The maximum cable length between IPBL and a single RFP must not exceed 1500 meters.

Note: Ensure that during the installation, each RFP is given an extra length (5-10 metres) of cable because it is possible that it will have to be moved for one reason or another.

1 Cut the cable to the correct length.

2 Connect the cable to a RJ45 modular jack. For information on the pinning, see below.

IMPORTANT: If local power supply is used for the RFP, the EPP cable pairs must NOT be connected.



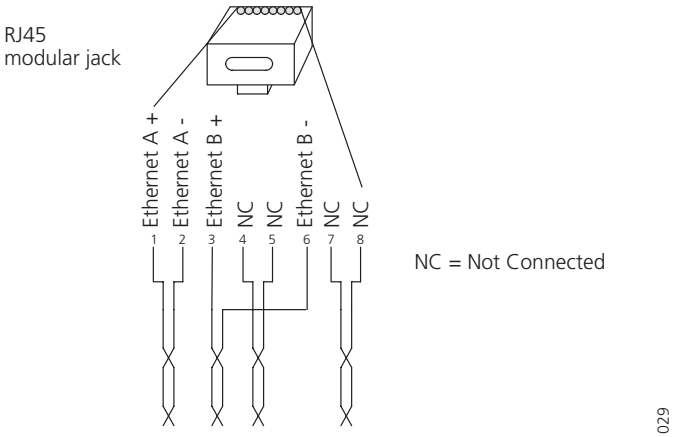
3 Label the cable.

6.2.3 LAN Cable

Note: The TX/RX crossover/straight cable feature does not work in the IPBL. It must be a straight cable between the IPBL and the switch port.

1 Cut the cable to the correct length.

2 Connect the cable to a RJ45 modular jack. For information on the pinning, see below.



3 Label the cable.

6.3 Power the IPBL

The IPBL power supply connectors are located at the rear. The power supply feeds both the IPBL and the connected RFPs. There are two alternatives to power the IPBL:

- 110/230 VAC, 60/50 Hz
- 48 VDC

6.3.1 110/230 VAC

The 110/230VAC (100 – 240 VAC) power input is protected against overload by a 4A fuse. The IEC 60320 type C14 (male) connector consists of:

- live lead (1)
- neutral lead (2)
- protective earth (3)

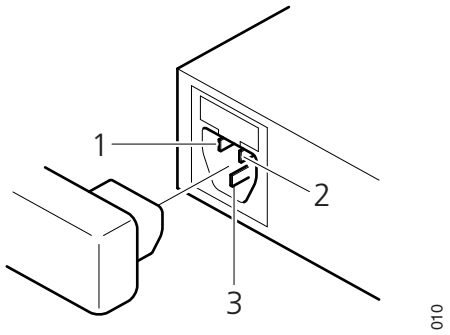


Figure 19. Pinning of the 110/230 VAC power supply

1 Connect the power cable on the IPBL.

2 Connect the power cable in a wall socket with protected earth.

The IPBL is switched on.

6.3.2 48 VDC

The 48 VDC (42 – 56 VDC) power input includes a fuse on the 48 VDC input to protect against overload. The IPBL also has a protection circuit to protect both the IPBL and the external power supply from damages caused by the user reversing the input terminals during installation.

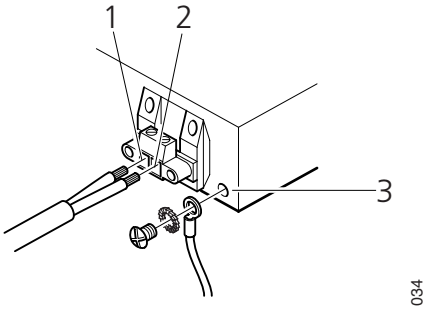


Figure 20. Pinning of the 48 VDC power supply

Note: A ground cable must be fastened to the protective earth (3) when 48 VDC is used as power source.

1 Fasten the ground cable to the protective earth (3) using the attached M4 screw (Philips) and washer.

2 Cut the power cable to the correct length.

The recommended wire size diameter is 1 mm (18 AWG).

3 Attach the positive lead to (1).

4 Attach the negative lead to (2).

5 Connect the power cable to 48 VDC power source.

7 Configuration

This section describes how to configure the IPBS and IPBL using the web interface. The recommended order to configure the equipment in the IP-DECT system is as follows:

1 Configure the Mobility Master, see 7.4 *Configure the Mobility Master* on page 50.

2 Configure the Standby Mobility Master, see 7.5 *Configure the Standby Mobility Master* on page 50.

3 Configure the Pari Master, see 7.6 *Configure the Pari Master* on page 51.

4 Configure the Standby Pari Master, see 7.7 *Configure the Standby Pari Master* on page 52.

5 Configure the Master, see 7.8 *Configure the Master* on page 52.

6 Configure the Standby Master, see 7.9 *Configure the Standby Master* on page 53.

7 Configure the Radios, see 7.11 *Configure the Radio* on page 54.

7.1 Requirements

The following is required in order to configure the IP-DECT system:

- PC
- 10/100base-T Ethernet connection

7.1.1 Web Browser Requirements

To use the interface properly, the web browser has to meet the following requirements:

- HTTP 1.1 protocol
- HTML 4.0 protocol
- XML/XSL Version 1.0

The GUI has been tested with Internet Explorer 7.x and Firefox 3.x, but can also be operated with other browsers in compliance with the requirements above.

7.2 Access the GUI

Note: To access the GUI for an IPBS/IPBL using secure web access (https), the certificate for the IPBS/IPBL can be installed in the web browser to avoid getting certificate error messages. See Appendix G: *Install Certificate in the Web Browser* on page 166.

The GUI interface is accessed through a standard web browser. It is possible to use the name, ipbs-xx-xx-xx and ipbl-xx-xx-xx, where xx-xx-xx is the end of the MAC address.

Note: The IPBL name is always ipbl-xx-xx-xx regardless if LAN1 (MAC xx-xx-xx-xx-xx) or LAN2 (MAC yy-yy-yy-yy-yy) is used.

It is also accessed by entering http://xxx.xxx.xxx.xxx. In this address, *xxx.xxx.xxx.xxx* should be replaced with the IP address determined in 7.2.1 *Determine the IP Address* on page 43.

Access the GUI and change the default password as described in 7.2.2 *Change the Default Password* on page 44.

Note: If the GUI cannot be accessed with Internet Explorer 8 or newer, check that the TLS 1.0 option is activated in the web browser under menu Tools > Internet Option > Advanced > Use TLS 1.0.

7.2.1 Determine the IP Address

The factory setting of the DHCP mode for the LAN1 port is "automatic", at first power up it will act as a DHCP client. If the network has a DHCP server, it will assign an IP address to the IPBS/IPBL. If there is no DHCP server in the network, the IPBS/IPBL can be assigned a predefined IP address. The factory setting of the DHCP mode is to the fixed IP address 192.168.0.1, see 8.2.1 Set 8.2.1 *Set DHCP Mode* on page 79.

Note: After the first startup the DHCP mode should be changed from "automatic" to either "client" or "off", see 8.2.1 *Set DHCP Mode* on page 79.

This section describes how to determine the dynamically allocated IP address. The address is used to access the IPBS/IPBL using a web browser. Two methods are described:

- *In a Network without a DHCP Server* on page 43.
- *In a Network with a DHCP Server* on page 43.

In a Network without a DHCP Server

If the network does not have a DHCP server, and the DHCP mode is set to "automatic" (factory default), follow the steps below.

Note: If the IPBS/IPBL has been used before, it must be restored to factory default settings by performing a long hardware reset, see 8.23 *Reset Using the Reset Button* on page 138.

1 Connect an Ethernet cable between the IPBS/IPBL and the computer.

NOTE: For IPBS, a power adapter must be used.
NOTE: For IPBL, make sure to use the LAN1 port.

2 Ensure that the computer has an IP address within the same IP address range as the IPBS/IPBL (192.168.0.1).

3 Perform a hardware reset by shortly pressing the reset button.
The IPBS/IPBL will be assigned the IP address 192.168.0.1 and the netmask 255.255.255.0.

4 Enter http://192.168.0.1 in the browser to access the IPBS/IPBL GUI.

5 After the first startup, do the following:
On the IPBS: Select LAN1 > DHCP
On the IPBL: Select LAN1 > DHCP

6 In *Mode* drop-down list, change the DHCP mode from "automatic" to "disabled".

In a Network with a DHCP Server

If the network has a DHCP server the IP address is determined following the steps below.

The IPBS's MAC address can be found on the label on the box and on the label on the backside. The IPBL's MAC address can be found on the label on the box. The hexadecimal numbers (xx-xx-xx-xx-xx-xx) represent the MAC address.

Note: Make sure to use the LAN1 port for the IPBL.

Note: In order to determine the IP address it is necessary that the computer is connected to the same LAN (broadcast domain) as the IPBS/IPBL.

Determine the IP address following the steps below:

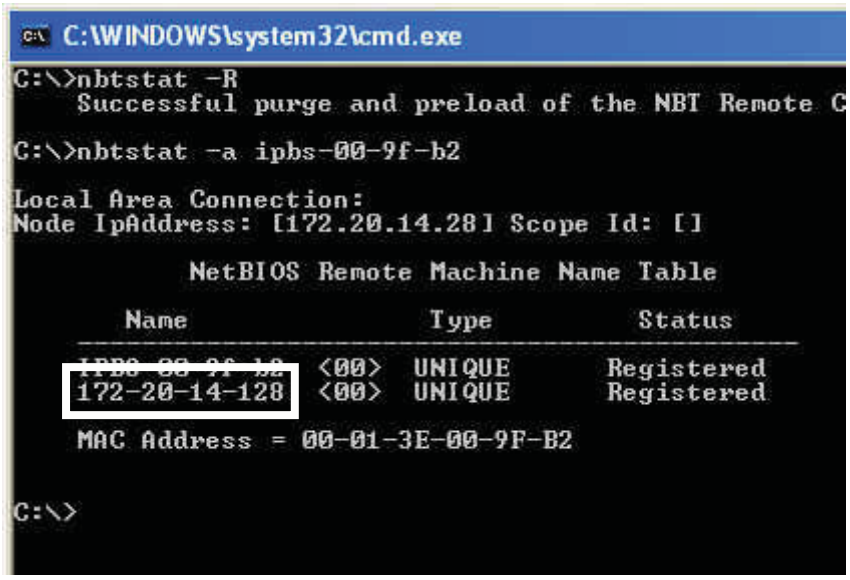
Note: If the IPBS/IPBL has been used before, it must be restored to factory default settings by performing a long hardware reset, see *8.23 Reset Using the Reset Button* on page 138. Then remove the power supply cable and connect it again.

1 Open a command window in windows by selecting Start > Run and enter "cmd" in the *Open:* text field.

2 Enter the following commands:
C:\ nbtstat -R
C:\ nbtstat -a ipbs-xx-xx-xx (in case of IPBL, enter "ipbl-xx-xx-xx")

Where xx-xx-xx should be replaced with the last 6 hexadecimal digits of the MAC-address.

3 The IP address is displayed in the command window, see the white frame in figure below.



4 Enter http://xxx.xxx.xxx.xxx (where *xxx.xxx.xxx.xxx* is the determined IP address) in the browser to access the GUI.

5 After the first startup of the IPBS/IPBL do the following:
On the IPBS: Select LAN1 > DHCP
On the IPBL: Select LAN1 > DHCP

6 In *Mode* drop-down list, change the DHCP mode from "automatic" to "client" or "disabled".

7.2.2 Change the Default Password

1 Enter the IP address determined in *7.2.1 Determine the IP Address* in the web browser address field.

2 Select General > Admin.

3 Enter user name and password in the dialog box.
Default user name is: admin.
Default password is: changeme.

4 Enter a user name in the *User Name* text field.

5 Enter a password in the *Password* text field. Repeat the password in the second text field.

6 Click "OK".

7.3 GUI Web Access

7.3.1 Login Page

When accessing IPBS/IPBL through a web browser the initial page is the login page. This page has two hyperlinks: *System Administration* and *User Administration*.

NOTE: Logging out of the IPBS/IPBL application is done by closing the web browser, to be completely logged out.

7.3.2 Access Levels

Three types of web users (or *Access Levels*) are authorized to access IPBS/IPBL:

- Auditors
- User Administrators
- System Administrators

The different types of access levels are described in the following table.

Access Level	Authorization	Login hyperlink on login page [a]	Described in section
Auditors	• Read access to device parameter settings • Can generate Service Reports	System Administration	*7.3.3 Auditors*
User Administrators	• Add, update and remove users	User Administration	7.3.4 *User Administrators* on page 46
System Administrators	• Write access to all device parameter settings (for example IP addresses, software upgrades) • Assign and modify access to other System Administrator and User Administrator account settings • Add, update and remove users	System Administration	7.3.5 *System Administrators* on page 47

a.Different users should use the hyperlink related to their access level. The system does not allow login by a link not related to the user's access level.

7.3.3 Auditors

Auditors have read access to device parameter settings but are not authorized to update those settings. Auditors are also allowed to generate Service Reports (Administration > Diagnostics > Service Reports).

The login steps for an auditor follow the steps of a normal system administrator login. See 7.3.5 *System Administrators* on page 47 for more information.

7.3.4 User Administrators

IPBS/IPBL is not supplied with preinstalled user administration accounts. Therefore, the first user administration account must be created by a system administrator (see 7.3.5 *System Administrators* on page 47). If additional user administration accounts are needed they must also be created by a system administrator, see *Managing User Administrators* on page 49.

User administrators can only administer users. They can view but not create or manage other user administrator accounts.

Login as User Administrator

To login as a user administrator:

1 Follow 7.2 *Access the GUI* on page 42 and access the device using a web browser.

2 Click the link labelled *User Administration.*

A login window is opened.

3 Enter user name and password for a user administrator.

4 Click "OK" to login.

5 Click the "Show" link.

6 The User Administration page is displayed.

See the figure below for a sample.

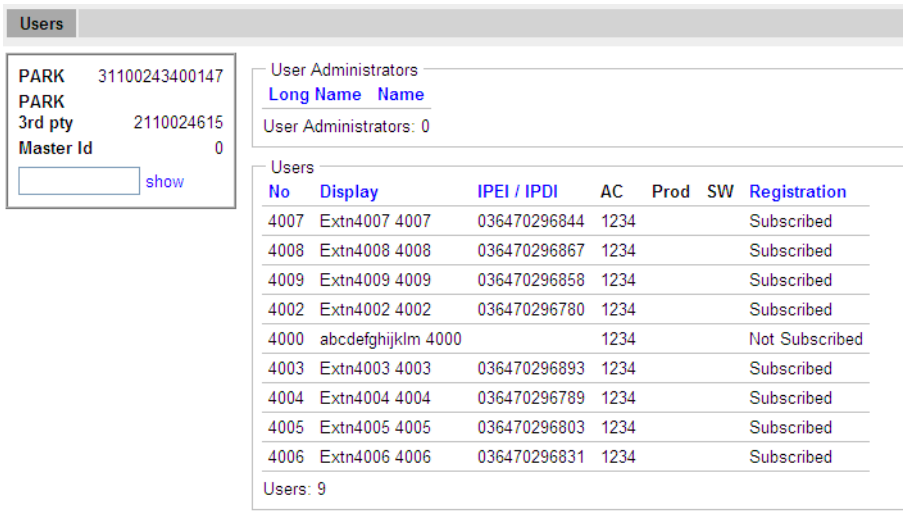


Figure 21. User Administration Sample.

The right side of the page consists of two list sections:

- *User Administrators* in the upper right section. **Note:** this section is read-only since a user administrator cannot manage other user administrators. See *Managing User Administrators* on page 49.
- *Users* in the lower right section. Refer to 7.13 *Add Users* on page 55.

7.3.5 System Administrators

IPBS/IPBL devices are factory delivered with a default system administrator account.

Log in as System Administrator

To login as a system administrator:

1 Follow 7.2 *Access the GUI* on page 42 and access the device using a web browser.

2 Click the link labelled *System Administration.*

A login window is opened.

3 Enter user name and password for a system administrator.

4 Click "OK" to login.

Following tasks can be done:

- Managing the default system administrator account, see *The Default System Administrator Account* on page 48.
- Managing additional system administrator accounts, see *Additional Administrator Accounts* on page 48.

The Default System Administrator Account

The default system administrator account can be modified but cannot be deleted. To modify the default system administrator account, do as follows:

1 Login as system administrator (see *Log in as System Administrator*).

2 Select General > Admin.

3 Select/Enter the following settings:

Field name	Description
• Device Name	Enter a description for the device.
• User Name	Enter a login user name.
• Password	Enter a password.
• Confirm Password	Confirm the password.

Note: Only changing the password will not result in the settings being saved. For the settings to be saved, both user name and password must be updated at the same time!

4 Click "OK".

Additional Administrator Accounts

Note: To create additional administrator accounts, Kerberos must have been configured (see 8.1.3 *Centralized Management of Administrator/Auditor Accounts Using Kerberos* on page 61).

To create an additional administrator account, do as follows:

1 Log in as system administrator (see *Log in as System Administrator* on page 47).

2 Select General > Kerberos

3 On the next free account row in the Users section:

- Enter User Name
- Enter Password
- Enter Password again
- Select *Administrator* (for System Administrator) or *Auditor* in the drop-down list (See 7.3.2 *Access Levels* on page 46 for a description of access levels.)

4 Click "OK".

The account row is created.

To modify an additional administrator account, do as follows:

1 Log in as system administrator (see *Log in as System Administrator* on page 47).

2 Select General > Kerberos

3 On an existing account row in the Users section::

- Enter a new user name
- Enter a new password
- Enter the password again
- Select *Administrator* (for System Administrator) or *Auditor* in the drop-down list (See 7.3.2 *Access Levels* on page 46 for a description of access levels.)

4 Click "OK".

The account row is updated.

To delete an additional administrator account, do as follows:

1 Login as system administrator (see *Log in as System Administrator* on page 47).

2 Select General > Kerberos

3 On the row to be deleted, select the *Delete* check box.

4 Click "OK".

The account row is deleted.

Managing User Administrators

Create a User Administrator

IPBS/IPBL is not supplied with preinstalled user administration accounts. Therefore, the first user administration account must be created by a system administrator. If additional user administration accounts are needed they must also be created by a system administrator.

1 Log in as System Administrator (see *Log in as System Administrator* on page 47).

2 Select "Users".

3 Click "show" .

The *User Administration* page (see figure 21 on page 47 for a sample) is displayed.

4 Click "new".

5 Select the "User Administrator" radio box. The window layout transforms.

6 Enter a long name.

7 Enter a name (NOTE: This field is used for login).

8 Enter a password.

9 Confirm the password.

10 Click "OK".

View and Modify a User Administrator

1 Login as System Administrator (see 7.3.5 *System Administrators* on page 47).

2 Select "Users".

3 Click "show".

A two-part list page is displayed. At the top are the user administrator accounts and below the user administrators are the user accounts, both listed in alphabetical order.

4 In the *User Administrators* section, click the hyperlink to be edited below the *Long Name* heading. An *Edit User* window is opened.

5 Select/Edit any of the following settings:

- Long Name
- Name (NOTE: This field is used for login)
- Password
- Confirm Password

6 Click "OK".

Delete a User Administrator

1 Login as System Administrator (see 7.3.5 *System Administrators* on page 47).

2 Select "Users".

3 Click "show".

4 In the *User Administrators* section, click the hyperlink to be deleted below the *Long Name* heading. An *Edit User* window is opened.

5 Click "Delete".

The User Administrator is deleted and the windows is closed.

7.4 Configure the Mobility Master

In a system with two or more Masters (Multiple Master system), a Mobility Master must be configured. For more information on Multiple Master Systems, see the applicable System Planning documentation for IP-DECT.

This section describes how to configure the Mobility Master. Each configuration step is briefly described in the step list below. For more detailed information see the corresponding subsection in 8 *Operation* on page 60.

1 Determine the address and access the GUI, see 7.2 *Access the GUI* on page 42.

2 Change the default password, see 7.2.2 *Change the Default Password* on page 44.

3 Set a static IP address and set DHCP to off, see 8.2.2 *Set a Static IP Address* on page 80.

4 Set the mode to Mobility Master, see 8.5.18 *Select Mobility Master Mode* on page 97.

5 Write a login name and enter a password, see 8.5.18 *Select Mobility Master Mode* on page 97.

6 Connect to other Mobility Master(s), see 8.5.19 *Connect Mobilty Master to other Mobility Master(s)* on page 98.

7 Enter the Time Server address, see 8.1.5 *Configure the NTP Settings* on page 68.

7.5 Configure the Standby Mobility Master

It is recommended to have a Standby Mobilty Master in a Multiple Master IP-DECT system. This section describes how to configure the Standby Mobility Master. Each configuration step is briefly described in the step list below. For more detailed information see the corresponding subsection in 8 *Operation* on page 60.

1 Determine the address and access the GUI, see 7.2 *Access the GUI* on page 42.

2 Change the default password, see 7.2.2 *Change the Default Password* on page 44.

3 Set a static IP address and set DHCP to off, see 8.2.2 *Set a Static IP Address* on page 80.

4 Set the mode to Standby Mobility Master, see 8.5.18 *Select Mobility Master Mode* on page 97.

5 Enter the primary Mobility Master IP address, see 8.5.18 *Select Mobility Master Mode* on page 97.

6 Enter a login name and enter a password, this must be the same as in the primary Mobility Master. See 8.5.18 *Select Mobility Master Mode* on page 97.

7 Connect to other Mobility Master(s). This should be the same Mobility Master(s) as in the primary Mobility Master, see 8.5.19 *Connect Mobilty Master to other Mobility Master(s)* on page 98.

8 Enter the Time Server address, see 8.1.5 *Configure the NTP Settings* on page 68.

7.6 Configure the Pari Master

This section describes how to configure the Pari Master. Each configuration step is briefly described in the step list below. For more detailed information see the corresponding subsection in 8 *Operation* on page 60.

1 Determine the address and access the GUI, see 7.2 *Access the GUI* on page 42.

2 Change the default password, see 7.2.2 *Change the Default Password* on page 44.

3 Configure LDAP user name and password, select the *Write Access* check box, see 8.4.1 *Configure LDAP Server* on page 82.

4 Set a static IP address and set DHCP to off, see 8.2.2 *Set a Static IP Address* on page 80.

5 Set the mode to Master, see 8.5.13 *Select Mode* on page 94.

6 Perform a reset to restart the IPBS/IPBL in Master mode, see 8.22 *Reset* on page 138.

7 Select system name and password, see 8.5.1 *Change System Name and Password* on page 89.

8 Change subscription method, see 8.5.2 *Set Subscription Method* on page 89.

9 Configure authentication code, see 8.5.3 *Configure Authentication Code* on page 90.

10 Select tones, see 8.5.4 *Select Tones* on page 90.

11 Set default language, see 8.5.5 *Set Default Language* on page 90.

12 Set frequency band, see 8.5.6 *Set Frequency Band* on page 90.

13 Enable carriers, see 8.5.7 *Enable Carriers* on page 91.

14 Enable local R-key handling, see 8.5.8 *Local R-Key Handling* on page 91.

15 Enable No transfer on hangup, see 8.5.9 *No Transfer on Hangup* on page 91.

16 Configure coder, see 8.5.10 *Configure Coder* on page 91.

17 Select supplementary services, see 8.5.12 *Configure Supplementary Services* on page 92.

18 Set Master Id, see 8.5.14 *Set Master Id* on page 94.

19 Enable Pari function, see 8.5.15 *Enable PARI Function* on page 94.

20 Enter gatekeeper IP address or ID, see 8.5.16 *Configure Gatekeeper* on page 95.

21 Connect to a Mobility Master, see 8.5.21 *Connect Master to a Mobility Master* on page 98.

22 Assign PARI, see 8.5.25 *PARI* on page 99.

23 Enter SARI, see 8.5.26 *SARI* on page 100.

24 Enter IMS3 IP address, see 8.7.1 *Configure Messaging* on page 103.

25 Enter the Time Server address, see 8.1.5 *Configure the NTP Settings* on page 68.

26 Reset in order to make the configuration changes take effect, see 8.22 *Reset* on page 138.

7.7 Configure the Standby Pari Master

It is recommended to have a Standby Pari Master in the IP-DECT system. This section describes how to configure a Standby Pari Master. Each configuration step is briefly described in the step list below, for more detailed information see the corresponding subsection in 8 *Operation* on page 60.

1 Determine the address and access the GUI, see 7.2 *Access the GUI* on page 42

2 Change the default password, see 7.2.2 *Change the Default Password* on page 44.

3 Configure LDAP replicator, enter the IP address, user name and password to the LDAP server (Pari Master). Alternative LDAP server must not be entered. Select the *Enable* check box, see 8.4.3 *Configure LDAP Replicator* on page 83.

4 Set a static IP address and set DHCP to off, see 8.2.2 *Set a Static IP Address* on page 80.

5 Set the mode to Standby Master, see 8.5.13 *Select Mode* on page 94.

6 Perform a reset to restart the IPBS/IPBL in Standby Master mode, see 8.22 *Reset* on page 138.

7 Enter system name and password, this should be the same system name and password as in the Pari Master, see 8.5.1 *Change System Name and Password* on page 89.

8 Select supplementary services, see 8.5.12 *Configure Supplementary Services* on page 92.

9 Set Master Id, see 8.5.14 *Set Master Id* on page 94.

10 Enable Pari function, see 8.5.15 *Enable PARI Function* on page 94.

11 Enter gatekeeper address, see 8.5.16 *Configure Gatekeeper* on page 95.

12 Connect to a Mobility Master, see 8.5.21 *Connect Master to a Mobility Master* on page 98.

13 Enter IMS3 IP address, see 8.7.1 *Configure Messaging* on page 103.

14 Enter the Time Server address, see 8.1.5 *Configure the NTP Settings* on page 68.

15 Reset in order to make the configuration changes take effect, 8.22 *Reset* on page 138.

7.8 Configure the Master

This section describes how to configure the Master. Each configuration step is briefly described in the step list below. For more detailed information see the corresponding subsection in 8 *Operation* on page 60.

1 Determine the address and access the GUI, see 7.2 *Access the GUI* on page 42.

2 Change the default password, see 7.2.2 *Change the Default Password* on page 44.

3 Configure LDAP user name and password, select the *Write Access* check box, see 8.4.1 *Configure LDAP Server* on page 82.

4 Set a static IP address and set DHCP to off, see 8.2.2 *Set a Static IP Address* on page 80.

5 Set the mode to Master, see 8.5.13 *Select Mode* on page 94.

6 Perform a reset to restart the IPBS/IPBL in Master mode, see 8.22 *Reset* on page 138.

7 Select system name and password, see 8.5.1 *Change System Name and Password* on page 89.

8 Set default language, see 8.5.5 *Set Default Language* on page 90.

9 Select supplementary services, see 8.5.12 *Configure Supplementary Services* on page 92.

10 Set Master id, see 8.5.14 *Set Master Id* on page 94.

11 Enter gatekeeper IP address or ID, see 8.5.16 *Configure Gatekeeper* on page 95.

12 Connect to a Mobility Master, see 8.5.21 *Connect Master to a Mobility Master* on page 98.

13 Enter IMS3 IP address, see 8.7.1 *Configure Messaging* on page 103.

14 Enter the Time Server address, see 8.1.5 *Configure the NTP Settings* on page 68.

15 Reset in order to make the configuration changes take effect, see 8.22 *Reset* on page 138.

7.9 Configure the Standby Master

It is recommended to have a Standby Master in the IP-DECT system. This section describes how to configure a Standby Master. Each configuration step is briefly described in the step list below, for more detailed information see the corresponding subsection in 8 *Operation* on page 60.

1 Determine the address and access the GUI, see 7.2 *Access the GUI* on page 42.

2 Change the default password, see 7.2.2 *Change the Default Password* on page 44.

3 Configure LDAP replicator, enter the IP address, user name and password to the LDAP server. Alternative LDAP server must not be entered. Select the *Enable* check box, see 8.4.3 *Configure LDAP Replicator* on page 83.

4 Set a static IP address and set DHCP to off, see 8.2.2 *Set a Static IP Address* on page 80.

5 Set the mode to Standby Master, see 8.5.13 *Select Mode* on page 94.

6 Perform a reset to restart the IPBS/IPBL in Standby Master mode, see 8.22 *Reset* on page 138.

7 Enter system name and password, this should be the same system name and password as in the Master. See 8.5.1 *Change System Name and Password* on page 89.

8 Select supplementary services, see 8.5.12 *Configure Supplementary Services* on page 92.

9 Set Master Id, see 8.5.14 *Set Master Id* on page 94.

10 Enter gatekeeper address, see 8.5.16 *Configure Gatekeeper* on page 95.

11 Connect to a Mobility Master, see 8.5.21 *Connect Master to a Mobility Master* on page 98.

12 Enter IMS3 IP address, see 8.7.1 *Configure Messaging* on page 103.

13 Enter the Time Server address, see 8.1.5 *Configure the NTP Settings* on page 68.

14 Reset in order to make the configuration changes take effect, see 8.22 *Reset* on page 138.

7.10 Plug and Play Configuration

Radios can be configured from the relevant Pari Master. When a new Radio is connected to the system, it automatically registers itself as an uninitialized registration to all Pari Masters in the system. It is possible to assign the Radio to one Pari Master. See *Add Radios* on page 108.

7.11 Configure the Radio

This section describes how to configure the Radio. Each configuration step is briefly described in the step list below, for more detailed information see the corresponding subsection in 8 *Operation* on page 60.

Note: When one Radio is configured, the configuration can be saved and uploaded to the other Radios in the system.

1 Determine the address and access the GUI, see 7.2 *Access the GUI* on page 42.

2 Change the default password, see 7.2.2 *Change the Default Password* on page 44.

3 Set DHCP mode to "Client", see 8.2.3 *Dynamic IP address via DHCP* on page 80.

4 Enable the Radio in the IPBS/IPBL, see 8.5.22 *Enable the Radio* on page 98.

5 Enter Pari Master and Standby Pari Master IP addresses, see 8.5.23 *Enter IP Address to the PARI Master and the Standby PARI Master* on page 99.

6 Configure air synchronization, see 8.5.27 *Configure Air Synchronization* on page 100.

7 Enter the Time Server address, see 8.1.5 *Configure the NTP Settings* on page 68.

8 Reset in order to make the configuration changes take effect, see 8.22 *Reset* on page 138.

9 Save the configuration of the Radio, see 8.14 *Backup* on page 126.

Configure the rest of the IPBSs/IPBLs following the steps below:

Note: Uploading the same configuration to all Radios can only be done if the DHCP is set to client.

1 Determine the address.

2 Select Update > Config and browse to the previously saved configuration. Click "OK".

3 Reset in order to make the configuration changes take effect, see 8.22 *Reset* on page 138.

4 Repeat step 1 to 3 for all Radios.

7.12 Configure Deployment

This section describes how to configure an IPBS for deployment used for coverage test of air sync and speech.

NOTE: For coverage test of air sync, two IPBSs must be configured, one as Sync Master and one as Sync Slave.

Each configuration step is briefly described in the step list below. For more detailed information see the corresponding subsection in 8 *Operation* on page 60.

1 Determine the IP address and access the GUI, see 7.2 *Access the GUI* on page 42.

2 Change the default password, see 7.2.2 *Change the Default Password* on page 44.

3 Set a static IP address and set DHCP to off, see 8.2.2 *Set a Static IP Address* on page 80.

4 Set the mode to Master, see 8.5.13 *Select Mode* on page 94.

5 Perform a reset to restart the IPBS/IPBL in Master mode, see 8.22 *Reset* on page 138.

6 Select system name and password, see 8.5.1 *Change System Name and Password* on page 89.

7 Set subscription method, see 8.5.2 *Set Subscription Method* on page 89.

8 Configure authentication code, see 8.5.3 *Configure Authentication Code* on page 90.

9 Select tones, see 8.5.4 *Select Tones* on page 90.

10 Set default language, see 8.5.5 *Set Default Language* on page 90.

11 Set frequency band, see 8.5.6 *Set Frequency Band* on page 90.

12 Enable carriers, see 8.5.7 *Enable Carriers* on page 91.

13 Set Master Id, see 8.5.14 *Set Master Id* on page 94.

14 Enable Pari function, see 8.5.15 *Enable PARI Function* on page 94.

15 Assign PARI, see 8.5.25 *PARI* on page 99. Note: If two IPBss are configured for coverage test of air sync, both IPBS must have the same system ID.

16 Enter SARI, see 8.5.26 *SARI* on page 100.

17 Reset in order to make the configuration changes take effect, see 8.22 *Reset* on page 138.

18 For coverage test of speech sync, register one handset in the IPBS configured as Sync Master, see 7.13 *Add Users* on page 55.

19 Set the mode to Deployment, see 8.5.13 *Select Mode* on page 94.

7.13 Add Users

This section describes how to add users to the IP-DECT system. The IPEI, which is the unique identification number of the handset, can be registered in three ways:

- Anonymous Registration can be used in en existing IP-DECT system. Instead of the administrator collects all the handset, the user of the handset does the registration. The IPEI is automatically associated to the user, see 7.13.1 *Anonymous Registration* on page 56.
- Individual Registration can be used if a few new handsets shall be added to the IP-DECT System. The IPEI is entered manually, see 7.13.2 *Individual Registration* on page 57.
- Easy Registration can be used if many users shall be added to the IP-DECT System. The IPEI is entered with for example a barcode reader to a csv file, see 7.13.3 *Easy Registration* on page 58.

Note: Display Name is only used during (AD) replication, see *Attribute Mappings* on page 85.

7.13.1 Anonymous Registration

Anonymous Registration is done in two steps. First, the user is registered in the IP-DECT System. Second, the handset is assigned to the user from the handset.

Add users in the IP-DECT System

1 Under *Administration*, select "Users".

2 Click "New".

3 Enter the following information in the corresponding text fields, leave the *IPEI* / *IPDI* text field empty, do not remove the automatically generated *Auth. Code*:

Field name	Description	Max. characters
• Long Name	Mandatory, the name of the user, need to be unique throughout the system.	30
• Display Name	Optional and only available when using the Ascom VoIP Gateway, the calling or called party name will be shown in the handset display (depending on whose handset).	30
• Name	Optional, the user name.	30
• Number	Mandatory, the phone number extension, need to be unique throughout the system.	30
• Password	Optional, is used for registration towards the gatekeeper.	30
• Idle Display	Optional, will be shown in the handset display when the handset is idle.	47

4 Click "OK".

5 Repeat step 2 to 4 for all users.

Assign Handsets to Users

1 Select DECT > System.

2 In the *Subscriptions* drop-down list, select "With System AC" to enable anonymous registration. Click "OK".

3 Perform an "over air subscription" using the system Authentication Code. For information on how this is done, see the reference guide of the handset.
The handset IPDI number appears in the Anonymous list. To view the list: Select Users > Anonymous.

4 Assign the handset to any user, subscribed or unsubscribed, on any Master defined in the system by calling the desired Master id & extension & optional individual AC code and hang up.
Example where **0** is the Master id, **200** is the extension and **1234** is the AC code: *0*200*1234#. If **200** is occupied by another handset, the new handset will be assigned this identity and the old handset will be moved to the anonymous list when logging in the new handset.
NOTE: When using AC code, start with * and end with # character. Otherwise skip the *# characters.

5 Repeat step 3 - 4 for all handsets.

Note: For safety reasons, when the Anonymous Registration is finished change the Subscription Method to "*Disable*" otherwise anyone could register to the IP-DECT System. See below for more information.

6 Select DECT > System.

7 Disable anonymous registration by selecting "Disable" in the Subscription drop-down list. Click "OK".

7.13.2 Individual Registration

1 Select DECT > System.

2 In the *Subscriptions* drop-down list, select "With System AC" or "With User AC". Click "OK".

Tip: See also 8.5.2 *Set Subscription Method* on page 89 for more information.

3 Select "Users".

4 Click "New".

5 Enter the following information in the corresponding text fields:

Field name	Description	Max. characters
• Long Name	Mandatory, the name of the user, need to be unique throughout the system.	30
• Display Name	Optional and only available when using the Ascom VoIP Gateway, the calling or called party name will be shown in the handset display (depending on whose handset).	30
• Name	Optional, the user name.	30
• Number	Mandatory, the phone number extension, need to be unique throughout the system.	30
• Password	Optional, is used for registration towards the gatekeeper.	30
• Idle Display	Optional, will be shown in the handset display when the handset is idle.	47
• IPEI / IPDI	Mandatory, the unique identification number of the handset.	
• Auth. Code	Optional, the individual authentication code for this user. Automatically created by default. Can be modified manually.	

6 Perform an "over air subscription" using the individual authentication code. For information on how this is done, see the reference guide of the handset.

7 Click "OK".

7.13.3 Easy Registration

Easy Registration is done in two steps. First, the users are registered in the IP-DECT System through an import of a csv file. Second, the handset is assigned automatically to the user from the handset.

Add users in the IP-DECT System

If many users should be added it is possible to import a csv file with the IPEI / IPDI.

Field name	Description	Max. characters
• Long Name	Mandatory, the name of the user, need to be unique throughout the system.	30
• Name	Optional, the user name.	30
• Number	Mandatory, the phone number extension, need to be unique throughout the system.	30
• Display Name	Optional and only available when using the Ascom VoIP Gateway, the calling or called party name will be shown in the handset display (depending on whose handset).	30
• Auth Name (SIP)	Optional	30
• Idle Display	Optional, will be showed in the handset display when the handset is idle.	47
• IPEI / IPDI	Mandatory, the unique identification number of the handset.	
• Password	Optional, is used for registration towards the gatekeeper.	15

The csv file may have the following format:

Long Name;Name;Number;Display Name;Auth Name (SIP);Idle Display;IPEI/IPDI;Password;

Different separators may be used in a delimiter-separated file. Import of files with the separators semicolon or TAB is supported.

1 Select Users.

2 Click “Import”.

3 Click “Browse” to locate the csv file.

4 Click Open > Next Make sure the correct number of entries are correct.

5 Click Next

Limitations

- Maximum 1000 rows in the csv file.
- The maximum csv file size is 128 Kb. If the file is to large, divide the file into several files.
- Only the new user data is imported. The old user data is not deleted.
- Existing user data cannot be updated.
- If the separator is wrong an error message will be displayed.

- The Authentication Code (AC) can not be entered in the csv file for safety reasons. The system generates a AC for every user in the list. If the user needs the AC the administrator will have to use Show, see 8.9.1 *Show all Registered Users in the IP-DECT System* on page 106.
- The Handset d41 and d62 must have version 3.2.X or later.
- The Handset d81 must have version 3.0.X or later.
- No other handsets in addition to the above works.

Assign Handset to Users

"With User AC" must be enabled, see 8.5.2 *Set Subscription Method* on page 89.

When the battery is inserted in the handset, the handset automatically connects to the IP-DECT system and assigns to the correct user.

8 Operation

This section describes the settings in the Configuration and Administration menu, each subsection represents a sub menu to the Configuration and Administration menu.

Some changes require a reset in order to take effect. It is possible to do several changes before resetting the IPBS/IPBL.

The GUI for the IPBS and IPBL are similar. Screen shots from the IPBS are used as default.

8.1 General

This section describes how to do the following configurations and settings.

- Name the equipment
- Change Administrator User Name and Password
- Kerberos
- Configure automatic firmware update
- Configure the NTP settings
- Configure Logging
- Configure the HTTP settings

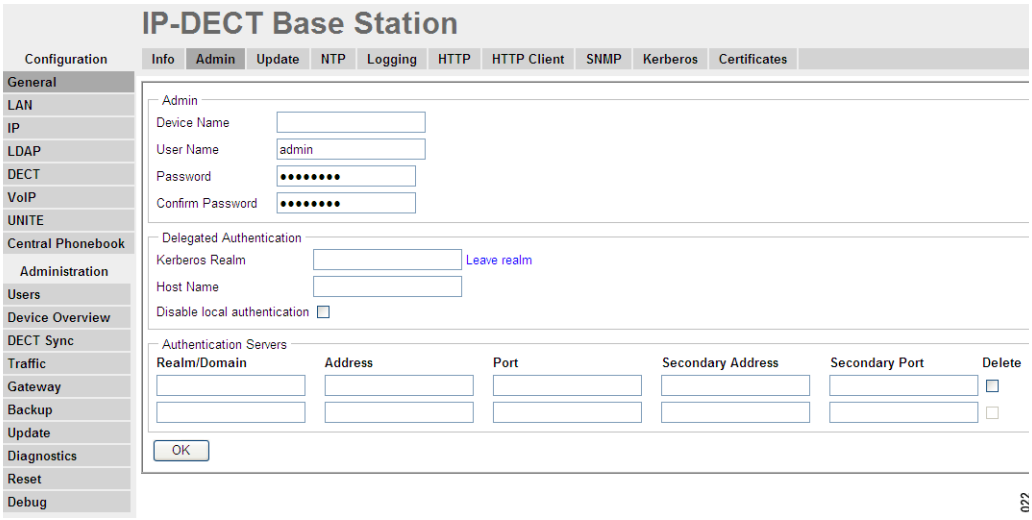


Figure 22. Assigning a administrator name, username, and password.

8.1.1 Name the IPBS/IPBL

Each IPBS/IPBL can be assigned a name. It is recommended to assign a descriptive name for example IPBS/IPBL location.

1 Select General > Admin.

2 Enter a name in the Device Name text field.

3 Click "OK".

8.1.2 Change User Name and Password

The user name and password are used to access the IPBS/IPBL through the web GUI.

1 Select General > Admin.

2 Write a user name in the User Name text field.

3 Enter a new password in the Password text field. Repeat the password in the second text field.

4 Click "OK".

8.1.3 Centralized Management of Administrator/Auditor Accounts Using Kerberos

In software version 3.x.x, each IPBS/IPBL had their own set of administrator/auditor accounts. Kerberos is a network authentication protocol that is used when you want to have the same set of user accounts for several IPBSs/IPBLs and then want to administrate these user accounts at one central location (Kerberos server). When an IPBS/IPBL is setup as a Kerberos server the IPBS/IPBL act as an authentication server for the rest of the IPBSs/IPBLs that are setup as client devices in the installation. The Kerberos server and the group of client devices constitute a domain called a realm. During Kerberos communication no password is actually sent over the network. Kerberos uses encrypted data packets (tickets) which are time-stamped and expire after a certain period of time. Therefore it is crucial to get the correct time across the system for which a NTP server should be used.

Set up the Kerberos server

It is recommended to set up the Kerberos server on the Master. To configure an IPBS/IPBL to act as a Kerberos server, do the following:

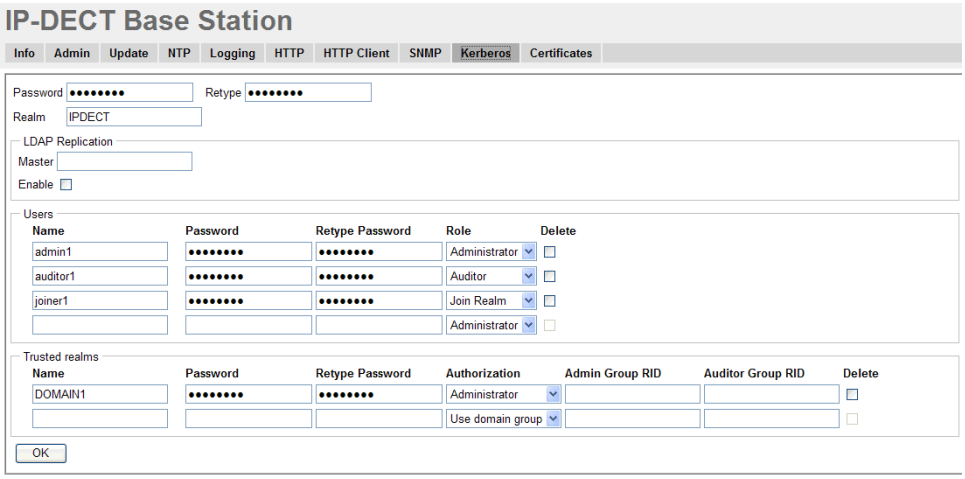


Figure 23. Configure Kerberos server

1 Make sure that the IP address of a NTP time server is specified. Select General > NTP.

2 Select General > Kerberos.

3 Enter a root password for the Kerberos server. This password is used to encrypt the information stored on the server.

4 Click "OK".

5 The Kerberos server is enabled. Enter the realm name of your choice in the *Realm* field. The Kerberos realms are typically written in upper-case letters.

6 Select/Enter the following information for the users of the realm.

Field Name	Description
Name	Enter a login user name
Password	Enter a password
Retype Password	Confirm password
Role	• Administrator: Write access to all device parameter settings • Auditor: Read access to device parameter settings • Join Realm: Add devices to the realm

7 Click "OK".

Set up the client

Depending on the type of system the IPBS/IPBL can be configured to act as a client in three different ways:

- Configure IPBS/IPBL as a client in a small existing system (few clients), see *Configure IPBS/IPBL as a client in a small existing system (few clients)*.
- Configure IPBS/IPBL as a client in a large existing system (many clients), see *Configure IPBS/IPBL as a client in a large existing system (many clients)* on page 63.
- Configure IPBS/IPBL as a client in a new system, see *Configure IPBS/IPBL as a client in a new system* on page 64.

Configure IPBS/IPBL as a client in a small existing system (few clients)

The location of the Kerberos server must be configured locally on each client. The server must be configured as a client as well so that it can also join the realm. To configure each IPBS/IPBL as a client, do the following:

1 Make sure that the IP address of a NTP time server is specified. Select General > NTP.

2 Select General > Admin.

3 Go to the *Authentication Servers* section.

4 In the *Realm/Domain* text field, enter the realm name specified in the Kerberos server.

5 In the *Address* text field, enter the IP address of the Kerberos server. In the Kerberos server enter 127.0.0.1 (localhost) as the IP address. The *Port* text field is filled out automatically.

6 Click "OK".

Join the realm

To enable delegated authentication using the Kerberos server, each client must join the Kerberos realm of the server. To join the realm, do the following:

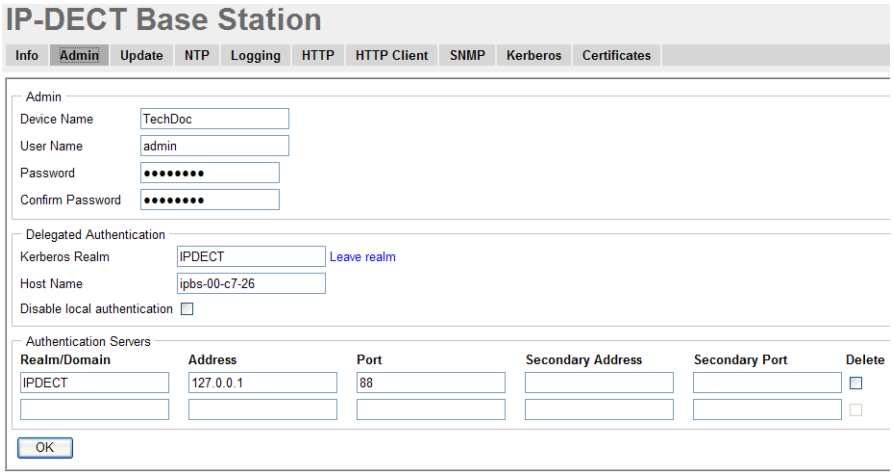


Figure 24. Configure the Kerberos client.

1 Select General > Admin.

2 Click on the blue text link "Join realm" in the *Delegated Authentication* section.

3 In the *Join Kerberos realm* window, enter the following in the text fields:
Realm: Enter the realm name of the Kerberos server.
Host name: The MAC address of the device. Default value is used.
Admin user name and Admin password: Enter the user name and password for a user with administrator account or join the realm account on the Kerberos server.

4 Click "Join".

Configure IPBS/IPBL as a client in a large existing system (many clients)

Precondition: All Masters and Radios are running on either software version 3.x.x or software version 4.1.x.

1 Install either the software version 4.1.x or software version 5.x.x using the update server and an update script, see 8.1.4 *Configure Automatic Firmware Update* on page 68.

2 Setup the update server using the update script described in *Appendix F*.

3 Select DECT > Radio config.

4 Go to the *Update* section.

5 In the *Command File URL* text field, enter the path to the update server and the name of the update script.

6 In the *Interval (min)* text field, enter the update period.

7 Click "OK".

After the script is executed and each Radio is restarted, the Kerberos client will join the Kerberos Server and it shall be possible to see all joined Kerberos clients in the bottom of the *Kerberos Server* tab.

The way the update script is done in *Appendix F: Update Script for Configuration of Kerberos Clients* it will automatically disable the local login possibilities if the joining was successful.

The password used in the script is now possible to change to a more secret password from the Kerberos server page.

It shall now be possible login to the Radio using the Kerberos login credentials, see *Log in using Kerberos* on page 64.

Configure IPBS/IPBL as a client in a new system

Precondition: The IPBS/IPBL must have software version 4.1.x or higher.

The idea is to use the *Device Overview -> Add* to configure the Radios and the Kerberos Client. By using this feature it is not needed to browse into each Radio for configuration.

The Radios are in broadcast mode which means none of them are attached to the Master and configured. If any of the Radios are attached to the master and configured, the Radios must be detached from the Master if this procedure shall work.

1 Select Device Overview > Radios.

2 Click "Add" to add the Radio to the Master.

3 In the *Add Radio* window, enter a name for the device. You can also add a Standby Master IP Address.

4 Go to the *Kerberos* section and enter the following in the text fields:
Realm: Enter the realm name of the Kerberos server.
Host name: Optional.
User: Enter the same user name defined in the Kerberos server.
Password: Enter the same password defined in the Kerberos server.
Disable local authentication: Select the *Disable local authentication* check box (recommended).
Overwrite existing: Select the *Overwrite existing* check box (optional).

5 Go to the *Authentication Servers* section.

6 In the *Realm/Domain* text field, enter the realm name specified in the Kerberos server.

7 In the *Address* text field, enter the IP address of the Kerberos server. In the Kerberos server enter 127.0.0.1 (localhost) as the IP address. The *Port* text field is filled out automatically.

8 Click "OK".

Log in using Kerberos

1 Make sure that secure HTTPS protocol is used when logging in.

2 Login on the client using a server account. When prompted for user name, the name of the realm has to be entered in front of the user name, separated by a backslash in the following way: REALM\username.

Disable local authentication

It is recommended to disable local authentication after Kerberos authentication is configured. It provides additional security and it is much easier to change the password of a user account or delete a compromises user account on the Kerberos server than changing the local user accounts on each IPBS/IPBL.

IMPORTANT: Make sure that the Kerberos authentication is working properly before disabling local authentication. If the Kerberos authentication is not working and local authentication is disabled it is not possible to access the IPBS/IPBL in any other way.

1 In the *Delegated Authentication* section select the *Disable local authentication* check box.

2 Click "OK".

Configure cross-realm authentication

Cross-realm authentication is used to authenticate users from another trusted realm. In this way it is possible for IP-DECT users to login to the IPBS/IPBL using their Windows user name and password in the Active Directory (AD). The trust relationship between the two realms is confirmed by configuring a shared password on both servers in the realms. This password is used to encrypt communication between the realms. To configure cross-realm authentication, do the following:

AD Server configuration for Windows 2003 servers

The trust relationship must be configured in the AD server.

1 In the Windows Start menu select Administrative Tools > Active Directory Domains and Trusts

2 Right-click the domain name and select "Properties".

3 Select the *Trusts* tab and click "New Trust...".

4 The *New Trust Wizard* appears. Click "Next".

5 Enter the name of the Kerberos realm. Click "Next".

6 Select "Realm trust". Click "Next".

7 Select "Nontransitive". Click "Next".

8 Select "One-way incoming". Click "Next".

9 Enter a password that will be a shared secret between the AD server and the Kerberos server. Click "Next".

10 Check the configuration and click "Next". Click "Finish".

Kerberos Server configuration

The trust relationship must also be configured in the Kerberos server.

1 Select General > Kerberos.

2 Select/Enter the following information in the *Trusted realms* section.

Field Name	Description
Name	Enter the name of the trusted Windows domain. Must be capital letters.
Password	Enter the shared password specified in the AD server
Retype Password	Confirm password

Authorization	Set user access rights from the Windows domain • Use domain group: Specify a Windows group with Administrator or Auditor rights • Administrator: All Windows domain users have administrator access rights • Auditor: All Windows domain users have auditor access rights
Admin Group RID	Specify the Relative Identifier (RID) of a Windows group with administrator rights. The RID is the last part of the Security Identifier (SID) of a group. Determine the SID of a group by entering the following in the Windows command line: whoami /groups This command displays the group information of the user logged in to the Windows domain.
Auditor Group RID	Specify the Relative Identifier (RID) of a Windows group with auditor rights. The RID is the last part of the Security Identifier (SID) of a group. Determine the SID of a group by entering the following in the Windows command line: whoami /groups This command displays the group information of the user logged in to the Windows domain.

3 Click "OK".

Kerberos Client configuration

The location of the Windows server must be configured locally on each client similarly to the Kerberos server. The client configuration must be done on the Kerberos server as well so that it can also join the Windows domain. To configure the clients, do the following:

1 Select General > Admin.

2 Go to the *Authentication Servers* section

3 In the *Realm/Domain* text field, enter the name of the trusted Windows domain.

4 In the *Address* text field, enter the IP address of the Windows server. The *Port* text field is filled out automatically.

5 Click "OK".

Log in using Kerberos cross-realm authentication

1 Make sure that secure HTTPS protocol is used when logging in.

2 Login on the client using a Windows server account. When prompted for user name, the name of the Windows domain has to be entered in front of the user name, separated by a backslash in the following way: DOMAIN\username.

Configure secondary Kerberos server

The Kerberos server is crucial when using Kerberos authentication, so it is recommended to have a secondary Kerberos server in the IP-DECT system. The secondary server is used if the primary server is not working properly. It is recommended to set up the secondary Kerberos server on the Standby Master. To configure an IPBS/IPBL as a secondary Kerberos server, do the following:

1 Make sure that the IP address of a NTP time server is specified. Select General > NTP.

2 Select General > Kerberos.

3 Enter the root password for the secondary Kerberos server which should be the same as the password used for the primary server. This password is used to encrypt the information stored on the server.

4 Click "OK".

5 The secondary Kerberos server is enabled. Enter the realm name in the *Realm* field.

6 LDAP is used to replicate the primary server database. Enter the IP address of the primary Kerberos server in the *Master* field in the LDAP Replication section. For more information about LDAP, see 8.4 *LDAP* on page 82.

7 Select the Enable check box.

8 Click "OK".

9 Click "OK" again to perform the LDAP replication.

Each client must also be configured with the secondary server information.

10 Select General > Admin.

11 Go to the Authentication Servers section.

12 In the Secondary Address text field of the Kerberos server, enter the IP address of the secondary Kerberos server. In the secondary Kerberos server enter 127.0.0.1 (localhost) as the IP address. The Port text field is filled out automatically.

13 Click "OK".

Delete a user or trusted realm

To delete a user account from the Kerberos server do the following:

1 Select General > Kerberos.

2 In the Users section select the Delete check box for the user to be deleted.

3 Click "OK".

To delete a trusted realm relationship from the Kerberos server do the following:

1 Select General > Kerberos.

2 In the Trusted Realms section select the Delete check box for the realm to be deleted.

3 Click "OK".

Deactivate Kerberos realm membership

IMPORTANT: Make sure that local authentication is enabled and working properly before leaving the Kerberos realm. If local authentication is still disabled and the IPBS/IPBL is no longer a member of the realm it is not possible to access the IPBS/IPBL in any other way.

1 Select General > Admin.

2 In the Delegated Authentication section clear the Disable local authentication check box.

3 Click "OK".

To deactivate the Kerberos membership for a client, do the following:

1 Select General > Admin.

2 Go to the Kerberos section and click on the blue text link "Leave realm".

3 It is possible to deactivate Kerberos realm membership in two ways:

- Deregister: The client is removed from the server database.
  In the *Leave Kerberos realm* window, enter the user name and password for a user with administrator or join the realm account in the *Deregister with Kerberos server* section.
  Click "Deregister".
- Delete: Leave the realm without removing data from the server.
  Click "Delete".

8.1.4 Configure Automatic Firmware Update

The IPBS/IPBL can be configured to automatically update its firmware. A script file must be uploaded to a suitable directory on an internal web server. For information on the script file syntax, see Appendix A: *How to Use the Update Server* on page 148.

1 Select General > Update

2 Enter the URL of the script file in the URL text field.

3 Enter the poll interval, in minutes, in the Interval (min) text field

4 Click "OK".

The Current Update Serials section shows the values of the variables set after the last execution of the associated command.

8.1.5 Configure the NTP Settings

Since the IPBS/IPBL does not have a battery-backed real-time clock, the internal time will be set to 0:00 hrs, 1.1.1970 in the case of a restart.

In order to get the correct time in the system, specify the IP address of a NTP time server. The IPBS/IPBL will synchronize its internal clock to the time server at startup and at the specified intervals. The clock is, for example, used by the handsets and log files.

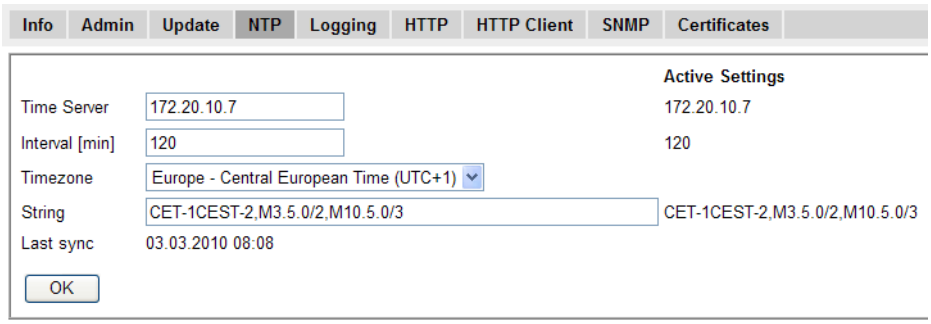


Figure 25. Configure NTP settings

1 Select General > NTP.

2 Enter the IP address to the primary NTP server in the *Time Server* text field.

3 Enter a time interval in the *Interval (min)* text field.

4 Select time zone in *Time zone* drop-down list. If the desired time zone is not in the list, select "Other" and edit the *String* text field following the instructions in the next step.

5 Enter the timezone string if automatically updates summer/winter is desired.

<String = StdOffset [Dst[Offset], Date/Time, Date/Time]>

- Std = Time zone (for example EST for Eastern Standard Time).
- Offset = time difference between the timezone and the UTC (Universal Time Coordinator).
- Dst = summertime zone (for example EDT for Eastern Daylight Time).
- Second Offset = time difference between the summer time and the UTC.
- Date/ Time, Date/ Time = beginning and end of summertime.
  - date format = Mm.n.d (d day of n week in the m month)
  - time format = hh:mm:ss in 24-hour format.

Note that a week always starts on a Sunday and the number for Sunday is 0.

Example:
North Carolina is located in the Eastern Time Zone. Eastern Standard Time (EST) is 5 hours behind UTC (StdOffset = EST-5), the Eastern Daylight Time (EDT) is 4 hours behind UTC (DstOffset = EDT-4). Summertime for the year 2006 begins at two a clock, on a Sunday, the first week in April (M4.1.0/2). The summertime ends at two a clock, on a Sunday, the fifth week in October (M10.5.0/2).

<String = EST-5EDT-4,M4.1.0/2,M10.5.0/2>

6 Click "OK".

8.1.6 Configure Logging

There are three ways to collect logs, see the table below.

TCP	The syslog entries are transmitted using a TCP connection.
SYSLOG	The entries are reported to a "syslogd" server in the network, which is responsible for further evaluation or storage of the entries.

HTTP	The syslog entries are transferred to a web server where they can be further processed. Each individual syslog entry is transmitted as form data to the web server in HTTP GET format.
HTTPS	The syslog entries are transferred to a web server where they can be further processed. Each individual syslog entry is transmitted as form data to the web server in HTTPS GET format.

Store the Syslog Entries using a TCP Connection

1 Select General > Logging
2 Select "TCP" in the *Type* drop-down list.
3 Enter the "IP address" of the logging server in the *Address* text field.
4 Enter the "Port" of the logging server in the *Port* text field.
5 Click "OK".

Store the Syslog Entries in a Syslogd

1 Select General > Logging.
2 Select "SYSLOG" in the *Type* drop-down list.
3 Enter the "IP address" of the syslogd in the *Address* text field.
4 Enter the desired syslogd message class in the *Class* text field.
5 Click "OK".

Store the Syslog Entries on a Web Server

1 Select General > Logging.
2 Select "HTTP" or "HTTPS" in the *Type* drop-down list.
3 Enter the IP address in the *IP Address* text field.
4 Enter the port in the *Port* text field.
5 Enter the relative URL of the form program on your web server in the *Path* text field.
6 Click "OK".

Note: The IPBS/IPBL will make an *HTTP GET* request or *HTTPS GET* request to the web server on the registered URL followed by the URL-encoded log entry.

Example:

Enter the value "/cdr/ cdrwrite.asp" in the "URL-Path" field if a page is on the web server with the name "/cdr/cdrwrite.asp" with a form that expects the log message in the "msg" parameter. In this example, the IPBS/IPBL will make a *GET /cdr/ cdrwrite.asp?event=syslog&msg=logmsg* request to the server.

Forward Alarms and Events

It is possible to forward alarms and events to a HTTP server destination. Typically this can be a Master base station. This programming can be done in the PARI Master (DECT > Radio config) or locally as described below.

1 Select General > Logging.

2 If the HTTP server destination requires HTTPS then select "HTTPS" in the *Type* drop-down list.

3 Enter the IP Address of the IPBS/IPBL where you want to have an overview of all faults in the External HTTP Server Address text field.

4 Enter the HTTP server port in the External HTTP Server Port text field. The default value is 80.

8.1.7 Configure the HTTP settings

Traditionally IPBS/IPBL has been administered over the network via the http protocol (default port 80).

In a secure system (see the IP Security chapter) IPBS/IPBL should be administered via the https protocol (default port 443). If for some reason port 443 is not to be used, you can use another port for the local https server and then access the IPBS/IPBL via this port.

Http and https traffic, respectively, would be disabled if their port values were to be set to zero (0). Therefore:

- To disable http traffic set "Port" to 0 (which is recommended in a secure system). Attempts to contact the device using the http protocol will result in an Unable to connect message.
- To disable https traffic set "HTTPS Port" to 0 (not recommended).

Any other port values would enable http and https traffic, respectively, for the port specified.

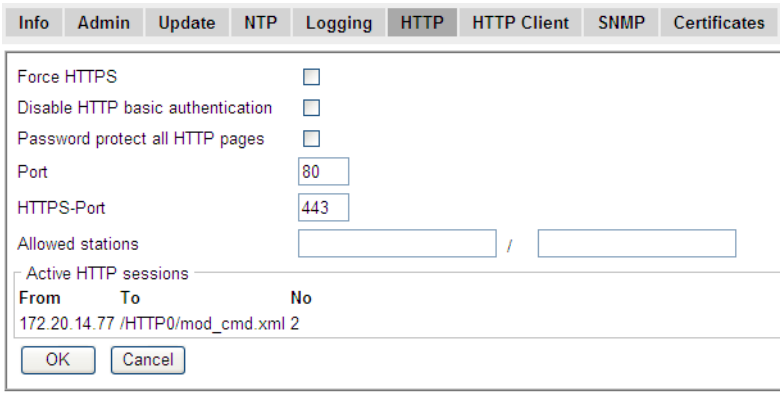


Figure 26. Configure the HTTP Settings

1 Select General > HTTP

- Select the Force HTTPS check box to allow only HTTPS sessions and all HTTP requests are redirected as HTTPS requests.
- Select the Disable HTTP basic authentication check box to require all administrative and programmatic clients to support HTTP digest authentication.
- Select the Password protect all HTTP pages check box to password protect all HTTP pages.
- Enter "Port number" in the Port text field. The IPBS/IPBL is by default administered over the network via the TCP port 80 (http). If port 80 is not to be used another port can be set up for access. Set this value to 0 to disable http

traffic (recommended). Attempts to contact the device using the http protocol will result in an Unable to connect message.
- Enter "HTTPS Port" in the HTTPS Port text field. To access IPBS/IPBL securely, use the TCP port 443 (https). Set this value to anything except zero (0) to enable https traffic. The default value is 443. The value zero (0) disables https traffic which is not recommended.
- Enter "Network Base Address" / "Network Base Mask" in the Allowed stations text fields to only allow access only from matching network, for example:172.16.0.0 / 255.255.0.0
- In the Active HTTP sessions field all ongoing HTTP traffic is displayed.

2 Click "OK".

8.1.8 Configure the HTTP Client settings

A list of URL that require authentication can be specified.

1 Select General > HTTP Client.

2 Enter the "URL" in the *URL* text field.

3 Enter "User" and "Password" in the *User* and Password text fields.

4 Click "OK".

A new row will be shown and more URLs can be added.

8.1.9 SNMP

Faults can be reported in the IP-DECT system via the Simple Network Management Protocol (SNMP). The SNMP framework has three parts:

- An SNMP manager: the system used to control and monitor the activities of network hosts using SNMP.
- An SNMP agent: the software component within the managed device that maintains data for the device and reports data, as needed, to managing systems.
- A MIB: The Management Information Base (MIB) is a virtual information storage area for network management information.

The agent and MIB reside on a network device (for example, router, access server, or switch). To enable the SNMP agent on the IPBS/IPBL, the relationship between the manager and the agent must be defined.

The MIB file can be downloaded from the Ascom's Extranet where the MIB file is included in the software package zip file.

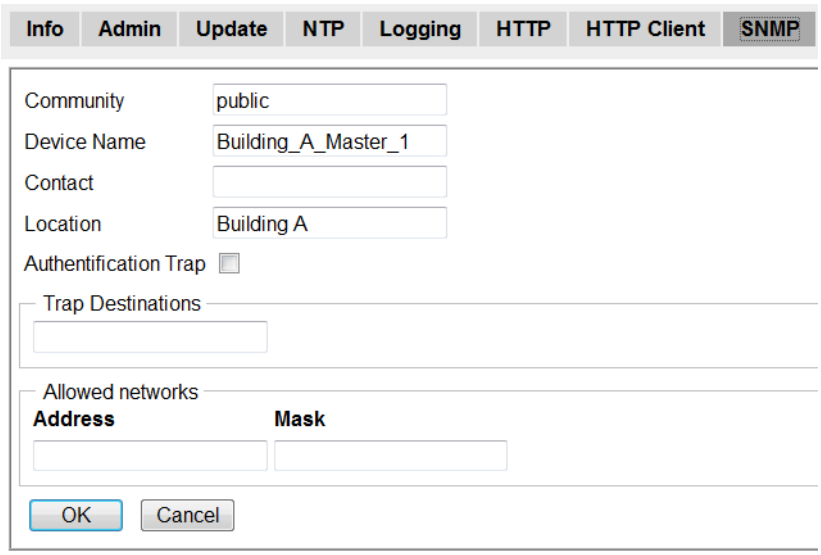


Figure 27. Configure SNMP Settings

1 Select General > SNMP

2 Enter a name in the Community field if you are not using the standard community name (public). The community text string acts like a password to regulate access to the agent on the Base Station.

3 Enter a device name in the Device Name field. This field is optional and serves only informational purposes.

4 Enter the name and phone number of the contact person in the Contact field. This field is optional and serves only informational purposes.

5 Enter a location in the Location field. This field is optional and serves only informational purposes.

6 Select the *Authentification Trap* check box to enable the sending of authentification traps. Access via SNMP is only possible if the correct Community Name is entered. If enabled a trap will be generated in the event of access with an incorrect Community Name.

7 Enter the IP address of the desired trap destinations in the *Trap Destinations* field. SNMP traps will be sent to all destinations.

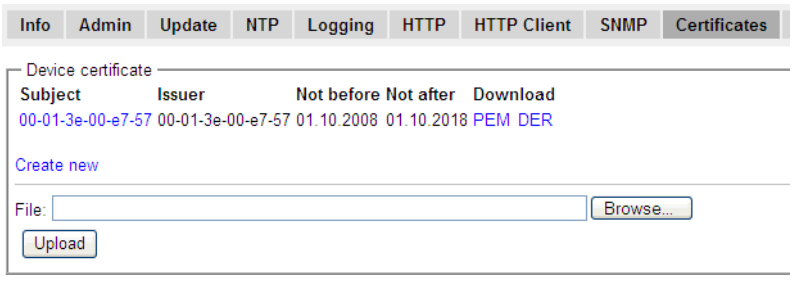
8 Enter the IP address and mask of the networks that are allowed to send SNMP requests. All networks are allowed if the field is empty.

9 Click "OK".

8.1.10 Certificates

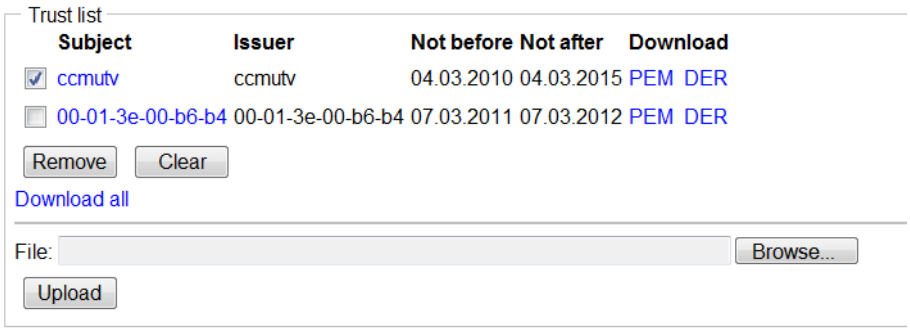
The Certificates tab is part of IP Security in IP-DECT. For more information on IP Security, see chapter 4 *IP Security* on page 22.

Select General > Certificates.



Trust List

A trust list is set up when the device must know which third parties (for example IP-PBX) it shall trust in. The list contains the certificates to be accepted by the device for TLS secured connections (for example HTTPS, SIPS).



The following table describes the different functions.

Field name	Description
• Subject	Click the hyperlink (under the Subject header) to display certificate details in a window.
• PEM	Click the PEM hyperlink (under the Download header) to download the certificate in PEM format.
• DER	Click the DER hyperlink (under the Download header) to download the certificate in DER format.
• Remove	To remove a certificate: Select the check box for the certificate and click the Remove button.
• Clear	To remove all certificates from the trust list: Click the Clear button.
• Download all	Click the Download all hyperlink (under the Remove button) to download the complete trust list as a PEM encoded text file.
• Upload	Use the Upload function to upload a certificate file to the device. 1 Click the Browse button 2 Select a certificate file 3 Click the Upload button to upload the file to the device.

Rejected Certificates

This list contains the certificate chains that were rejected before, while trying to establish a secure TLS connection. This happens for example if the certificate is expired or neither the certificate nor any of the issuing CAs is trusted. If one of that certificates should be trusted for future connections you can select and add it to the trust list, directly.

The following table describes the different functions.

Field name	Description
• Subject	Click the name of a certificate to display its details in a window.
• Clear	Discard all rejected certificate chains.
• Trust	Click this button to add the selected certificates to the trust list and remove the corresponding chains from the rejected certificates..

Device Certificate

As described in *2. Certificate Handling Options with Device Certificates* on page 24, there are three possible certificate options:

1 Default device certificate, see *Default Device Certificate* on page 76.

2 Self-signed certificates, see *Self-signed Certificates* on page 76.

3 Certificates signed by a Certificate Authority (CA), see *Certificate Signing Request (CSR)* on page 77.

The following table describes the different functions.

Field name	Description
• Subject	Click the hyperlink (under the Subject header) to display certificate details in a window.
• PEM	Click the PEM hyperlink (under the Download header) to download the certificate in PEM format.
• DER	Click the DER hyperlink (under the Download header) to download the certificate in DER format.
• Trust	Click this button to add the selected certificates to the trust list.
• Clear	This button is only displayed if a certificate was installed by the user, before. Click this button to discard the current device certificate and restore the standard certificate.
• Create New	The Create New hyperlink is used for two purposes: • *Self-signed Certificates* on page 76 • *Certificate Signing Request (CSR)* on page 77

- Upload

  Use the Upload function to upload a certificate file to the device.

  1 Click the Browse button

  2 Select a certificate file

  3 Click the Upload button to upload the file to the device.

  NOTE: The Upload function requires a previously issued CSR to exist.

Default Device Certificate

This section corresponds to option 1 in *2. Certificate Handling Options with Device Certificates* on page 24.

If the default device certificate is missing for the device it will be generated, together with a key pair, when the IPBS is upgraded to version R3. The default certificate contains the MAC address of the device and will be valid for 10 years.

If the self-signed certificate is deleted and the device is restarted, a new certificate and key pair will be generated.

HTTPS is deactivated during the generation (creation) of the certificate.

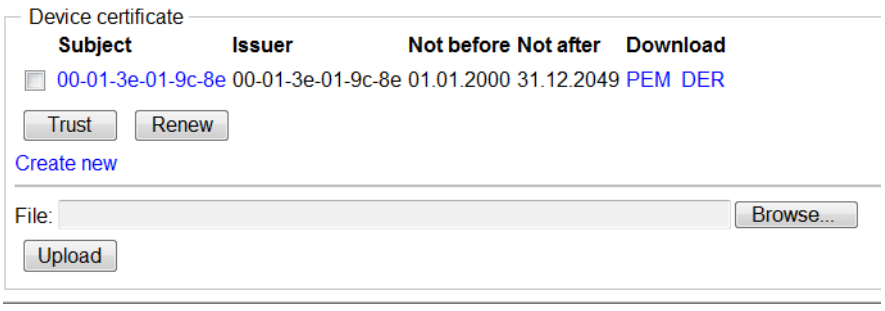
The default certificate is a self-signed certificate. This means that certificates cannot be verified and thus the user/administrator will be prompted by the web browser to accept the certificate before it can be used. From this point on within the browser session (as long as the certificate is not changed) communication between the browser and the device is possible without further accept operations from the user/administrator.

If the device certificate is replaced or regenerated the user/administrator has to manually accept the new certificate.

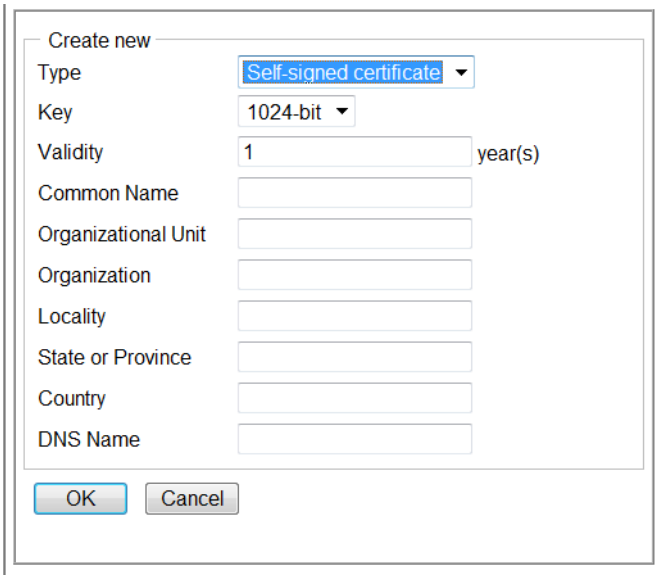
Self-signed Certificates

This section corresponds to option 2 in 4.2.2 *TLS Certificates* on page 24.

1 Select Configuration > General > Certificates.



2 Click the "Create New" hyperlink in the *Device Certificate* section. A *New Certificate* window opens.



3 Select "Self-signed certificate" in the *Type* drop-down list.

4 Select/Enter the following settings:

Field name	Description
• Validity	Enter the default validity in years. This is a mandatory field.
• Key	Select either the desired key strength (1024-bit, 2048-bit, 4096-bit) or select to reuse the old key pair (this is not recommended).
• Common Name	Enter the domain name or IP address for the device. This is the same value as entered in the web browser when accessing the device.
• DNS Name	If the device has got a DNS name it should be entered here. It will be stored as a subjectAltName (SAN) in the certificate. The format of this field is a FQDN (e.g. host.domain.com).

5 Click "OK".

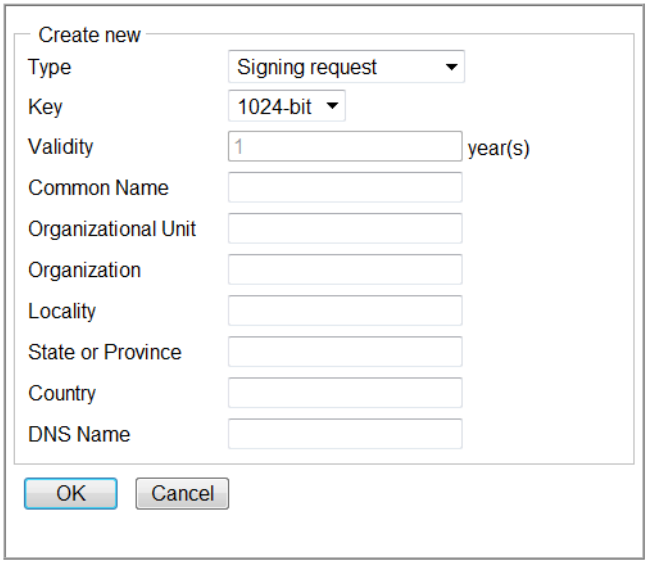
6 A new key pair and a certificate will be created. This may take up to one hour depending on the key strength selected. During this time the device will be fully operational with the exception of https not working and the certificate tab pane not being visible.

Certificate Signing Request (CSR)

This section corresponds to option 3A & 3B in 4.2.2 *TLS Certificates* on page 24. This will be the most common options for IP-DECT systems. For more information on CSRs see *Certificate Authorities* on page 22.

1 Select Configuration > General > Certificates.

2 Click the "Create New" hyperlink in the *Device Certificate* section. A *New Certificate* window will open.



3 Select "Signing Request" in the *Type* drop-down list.

4 Select/Enter the following settings:

Field name	Description
• Validity	This is an read-only information field indicating a default mandatory validity of 1 year. The time length of the validity is defined by the CA.
• Key	Select the desired key strength (1024-bit, 2048-bit, 4096-bit) or select to reuse the old key pair (this is not recommended).
• Common Name	Enter the domain name or IP address for the device. This is the same value as entered in the web browser when accessing the device.
• DNS Name	If the device has got a DNS name it should be entered here. It will be stored as a subjectAltName (SAN) in the certificate. The format of this field is a FQDN (e.g. host.domain.com).

5 Click "OK". The windows closes.

A key pair and a CSR file will be created. This may take up to one hour depending on the key strength selected. During this time the device will be fully operational with the exception of https not working and the certificate tab pane not being visible.

When the CSR file has been generated it is visible in the Signing Request section of the Certificates page.

6 Download the CSR file by clicking the "PEM" or "DER" link in the *Signing Request* section.

7 Send the CSR file to your CA.

8 If successful your CA will send back a digitally signed certificate file. This file should now be uploaded.

9 Select the certificate file.

10 Click "Upload".

Note: If the CSR file generated in step 5 is deleted before receiving the reply from the CA (in step 8) it will not be possible to upload the signed certificate file in step 10. The system will automatically delete the CSR file when step 10 has completed.

8.1.11 License

Select Configuration > General > License.

Licenses are used to activate additional functions in the IP-DECT system. Which functions that are activated are depending on type of license.

Do as follows:

1 In the License Key field: Enter a license number.

2 Click "OK".

8.2 LAN

This section describes how to do the following configurations and settings.

- Set DHCP mode
- Set IP static address
- Set dynamic IP address
- Set link type
- Configure VLAN
- View LAN statistics
- Deactivate LAN port (only for IPBL)

Note: The IPBL has two LAN ports. LAN1 port must be used in the IP-DECT system (LAN2 port is for administration only).

8.2.1 Set DHCP Mode

The IPBS/IPBL can have different DHCP modes, see the table below.

Disabled	Used if the IPBS/IPBL should have a static IP address.
Client	The IPBS/IPBL acts as a DHCP Client, if there is a DHCP server in the network it will be assigned an IP address
Automatic	In automatic DHCP mode the IPBS/IPBL will act as a DHCP client on power up. If the IPBS/IPBL is restarted by shortly pressing the reset button it will get the IP address 192.168.0.1 and the netmask 255.255.255.0 for the LAN1 port.

Change DCHP mode following the steps below.

1 On the IPBS: Select LAN > DHCP.
On the IPBL: Select LAN1 > DHCP.

2 Select DCHP mode in the *Mode* drop-down list.

3 Click “OK”.

4 If "Client" or "Automatic" is set, reset to make the changes take effect. See 8.22 *Reset* on page 138.

8.2.2 Set a Static IP Address

It is necessary for the Master and the Standby Master to have static IP addresses. The Radios can have dynamic IP addresses retrieved from the network DHCP server.

Ask the network administrator to reserve an IP address for the Master and Standby Master.

1 On the IPBS: Select LAN > DHCP.
On the IPBL: Select LAN1 > DHCP.

2 Select "Disabled" in the *Mode* drop-down list.

3 Click "OK".

4 Do NOT reset the device yet. Set a static IP address first.

1 On the IPBS: Select LAN > IP.
On the IPBL: Select LAN1 > IP.

2 Enter "IP Address", "Network Mask", "Default Gateway" and "DNS Server" addresses provided by the network administrator in the text fields.

You can also enter an alternative DNS Server in the Alt. DNS Server text field and select the Check ARP check box to detect and prevent ARP poisoning attacks.

3 Click "OK".

4 Reset in order to make the changes take effect, see 8.22 *Reset* on page 138.

5 Start the web-based configuration, using the static IP address.

8.2.3 Dynamic IP address via DHCP

The Radios can have dynamic IP address allocation if the network has an DHCP server.

1 On the IPBS: Select LAN > DHCP.
On the IPBL: Select LAN1 > DHCP.

2 Select "Client" in the *Mode* drop-down list.

3 Click "OK".

4 Reset in order to make the changes take effect, see 8.22 *Reset* on page 138.

Note: If the DHCP lease time is shorter than the time-to-live of the name/IP address association in the Windows Internet Name Service (WINS) server, it may cause a mismatch, and a wrong device may be reached if its WINS name is used.

8.2.4 Link

1 On the IPBS: Select LAN > Link.
On the IPBL: Select LAN1 > Link.

The link setting should be set to "auto" under all normal circumstances.

8.2.5 Configure VLAN

Identity and priority settings for VLAN are done in the "LAN > VLAN" sub menu.

Note: It is necessary to have a VLAN with the same ID as configured in the IPBS/IPBL, otherwise it will not be possible to access the IPBS/IPBL.

Note: If "VLAN = 0", the Quality of Service (QoS) is inactive according to 802.1q.
It is also recommended to avoid "VLAN = 1" as it often is used as a default VLAN setting.

8.2.6 View LAN Statistics

To view statistics of LAN events:

1 On the IPBS: Select LAN > Statistics.
On the IPBL: Select LAN1 > Statistics.

To reset the ethernet statistics counters, click "Clear".

8.2.7 Deactivate LAN Port (only for IPBL)

To deactivate LAN port:

1 Select LAN2 > IP.

2 Select the Disable check box.

3 Click "OK".

The LAN2 port is for administration only and it is the port you in normal case are interested in deactivating.

8.3 IP

8.3.1 Configure IP Settings

The following settings can be done in the IP settings sub menu:

ToS priority, RTP Data and VoIP Signalling:	Determines the priority from the ToS field in the IP header. This function can be used if the router can use ToS priority control. Hexadecimal, octal or decimal values can be used; 0x10, 020 and 16 are all equivalent. There are two fields for ToS priority, one for RTP Data and one for VoIP Signalling[a]. Other types of traffic (for example http and ldap) are not prioritized and use 0x00. NOTE: Remember that the same value should be set in the ToS field for all devices.
RTP ports:	If the ports fields are left blank, the ports 16384 to 32767 will be used.

a. VoIP Signalling includes roaming, handover, registrations towards the IP-PBX etc.

1 Select IP > Settings.

2 Enter the ToS priority value (recommended value is "0xb8") in the ToS Priority - RTP Data text field.

3 Enter the ToS priority value (recommended value is "0x68") in the *ToS Priority - VoIP Signalling* text field.

4 Select which ports to use for RTP traffic by entering the first port in the First UDP-RTP Port text field.

5 Enter the number of ports to use in the Number of Ports text field.

6 Click "OK".

8.3.2 Routing

View the IP routing by Select IP > Routing.

8.4 LDAP

The Lightweight Directory Access Protocol (LDAP) protocol is required for systems in which the server and a replicating client access a joint user database. All IPBSs/IPBLs in the system have access to the database, one of the IPBSs/IPBLs can be configured to be the LDAP server.

The joint user database contains information about the users registered in the system. It also contains the system configuration, that is the configurations made under the *DECT* menu.

This section describes how to do the following configurations and settings.

- Configure LDAP Server
- Check LDAP Server Status
- Configure LDAP Replicator
- Check LDAP Replicator Status

8.4.1 Configure LDAP Server

The IP-DECT system needs an LDAP server in some configurations. If the VoIP gateway is set up as an LDAP server, the Master should be set up as an LDAP replicator, see 8.4.3 *Configure LDAP Replicator* on page 83.

Setup the IPBS/IPBL as an LDAP server

Note: The selected user name and password must be the same in both the Master and the Standby Master. If a Multi Master system is used, the Masters must also have the same user name and password.

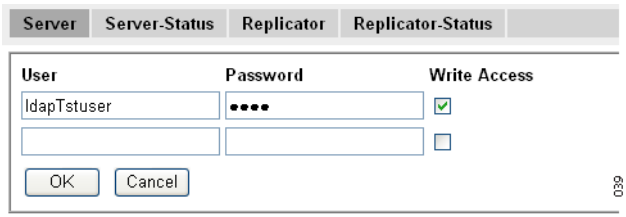
1 Select LDAP > Server.

2 Add a user, for example ldap-user, in the *User* text field.

3 Enter a password in the *Password* text field.

4 Select the *Write Access* check box.

5 Click "OK".



8.4.2 Check LDAP Server Status

Select LDAP > Server Status

The following information is displayed:

- connections - Total number of active connections to the LDAP server

- write connections - Number of write-enabled connections
- rx search - Number of received search requests
- rx modify - Number of received change requests
- rx add - Number of added objects
- rx del - Number of deleted objects
- rx abandon - Number of lost connections
- tx notify - Number of sent change notifications
- tx error - Number of sent error notifications
- tx error 49 - Number of sent error notifications due to invalid credentials
- tx error 50 - Number of sent error notifications due to insufficient access rights

8.4.3 Configure LDAP Replicator

LDAP Replicators are usually configured in the following cases:

- User data is replicated from the Master to the Standby Master. The replicator is configured on the Standby Master (Full Directory Replication)
- User data is replicated from the Active Directory (AD) to the Master. The replicator is configured on the Master
- User data is replicated from the PBX to the Master. The replicator is configured on the Master (Full Directory Replication)
- User data is replicated from the Master to the other Masters in a Multi Master System. The replicator is configured on the Masters not hosting the LDAP Server. To have full roaming between Masters, the LDAP user must have write access to the LDAP server.

Configure Full Directory Replication

1 Select LDAP > Replicator.

2 Select "Full Replication" in the *Type* drop-down list.

3 Select the *Enable* check box.

4 Enter the IP address to the LDAP server in the *Server* text field.

5 Enter the IP address to the alternative LDAP server in the *Alt. Server* text field.

6 NOTE: If this IPBS/IPBL is configured as an alternative/standby LDAP server, leave the *Alt. Server* text field empty.Select a filter method from the *Filter Type* drop-down list

   - Dect Gateway Name - Enter the name of the DECT gateway to limit the replication to users of a certain group
   - LDAP Filter - Enter an LDAP filter to limit replication to certain LDAP objects

7 Enter the LDAP User name and Password in the *User* and *Password* text fields.

8 Click "OK".

Note: In the case of Master to Standby Master Full Directory Replication, do not register new handsets when the LDAP Server is down even if there is a Standby LDAP Server in the system.

Configure Active Directory Replication

During Active Directory (AD) replication the configured LDAP replicator retrieves only relevant data.

AD replication is a one-way replication where data is only transferred from the AD to the IP-DECT but not from the IP-DECT to the AD. Data originating from the AD cannot be

modified in the IP-DECT system, but it is possible to change or add those user attributes locally that are not replicated.

Note: If AD replication is enabled, existing local users are replaced with corresponding users in the AD, and some local attributes may be deleted. Contact Ascom Technical Support if you would like to enable AD replication with existing local users.

For AD Server configuration settings, see *Configure AD Server* on page 87.

1 Select LDAP > Replicator.

2 Select "Active Directory Replication" in the *Type* drop-down list.

3 Select the *Enable* check box.

4 Enter the IP address to the AD in the *Server* text field.

5 Enter a Distinguished Name (DN) to configure a search base for AD users.

The user information is usually replicated so It is recommended to write "CN=Users, DC=DomainName" where "DomainName" is the name of the domain on the AD server.

You can also click "Show Options..." to see some naming contexts on the configured server.

6 Enter an LDAP filter to retrieve only the relevant LDAP objects from the AD.

A default (objectclass=user) filter is offered, but it is recommended to assign all IP-DECT users to a group within the AD. For example, the following filter can be entered to retrieve only IP-DECT users.

"(&(objectClass=user)(memberOf=CN=grp_ipdect,CN=Users,DC=DomainName))"

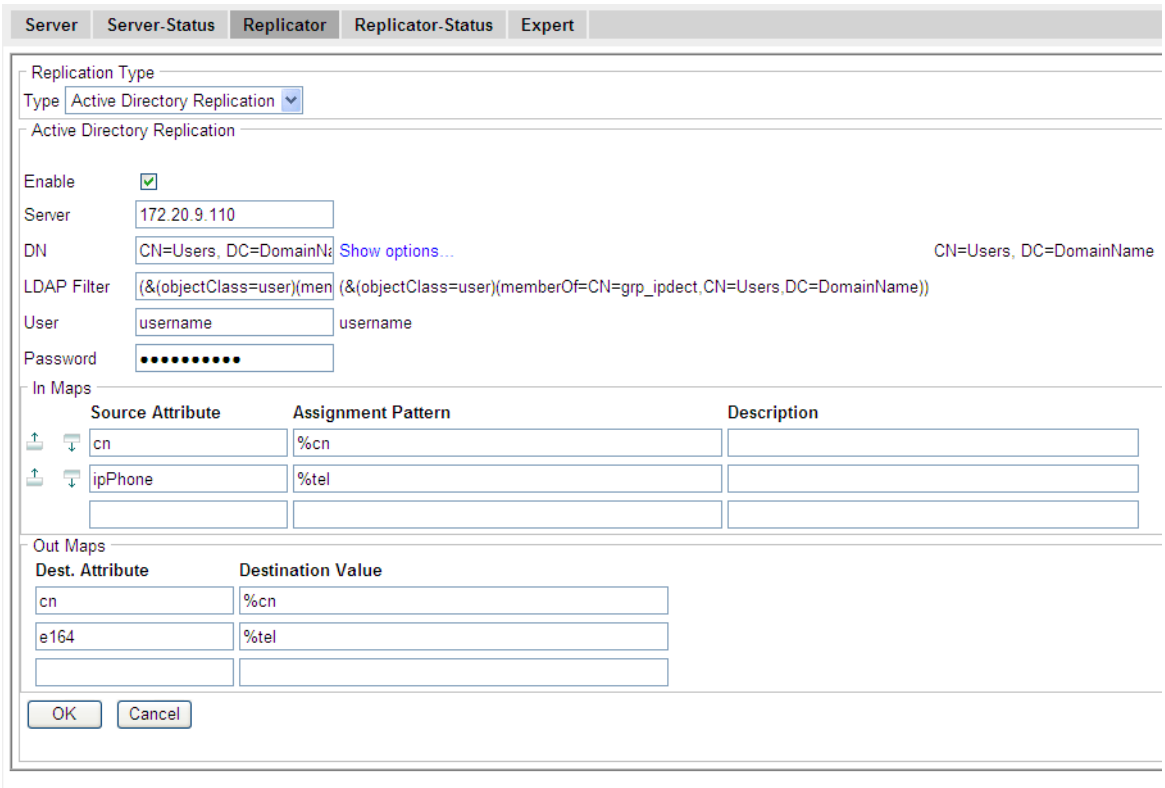
where "grp_ipdect" is the group created for IP-DECT users, "Users" is the default folder for users and "DomainName" is the name of the domain on the AD server.

7 Enter the user name and the password of a user who has read access to the AD in the *User* and the *Password* text fields. It is recommended to choose a user with Enterprise Administrator rights.

8 Configure In Maps and Out Maps for Attribute mapping. Attribute mapping describes how the obtained information from the AD is handled within the IP-DECT system. For more information see *Attribute Mappings* on page 85.

9 Click "OK".

10 After proper configuration check the Replicator Status by selecting LDAP > Replicator Status. The state of the Active Directory Replication should be "Up" and the state of the remote directory should be "Completed".



Attribute Mappings

The following attributes are generally used to configure attribute mappings:

IP-DECT designator	IP-DECT attribute name	AD attribute name	Description
Long Name	cn	cn	Common name, mandatory and must be unique
Name	h323	userPrincipalName	User name
Number	e164	telephoneNumber, ipPhone, mobile	Business or mobile phone number, mandatory and must be unique
Display	dn	displayName, givenName, sn	Displayed name, first name or surname

In Maps

In Maps define which attributes of the incoming objects are replicated and how the attributes are used in the IP-DECT system. In Maps can be configured with the following text fields:

- Source Attribute - The name of the AD attribute to be replicated. Only those users are replicated who have the defined source attributes. See *AD attribute name* on page 85 for examples.

- Assignment Pattern - A regular expression that assigns AD attributes to local temporary variables. A local temporary variable can have any name starting with a % sign, for example %tel. Regular expressions are written in a formal language that is widely used in Unix environments. For more information, see regular expression manuals on the internet.
- Description - Short explanation of what is configured with regular expressions

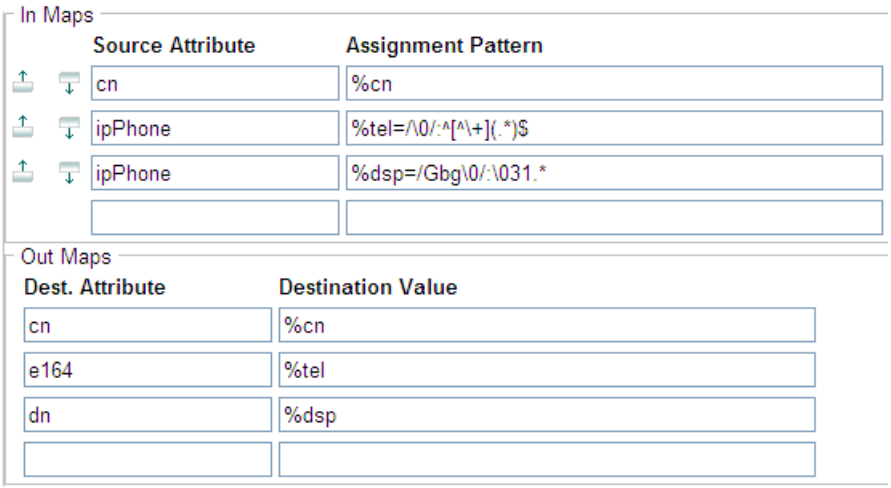
If there are several in maps for one attribute, all maps are handled in the order of appearance. To change the order of appearance click the "Move Up" or "Move Down" icons on the left side of the *In Maps* window.

Out Maps

Out Maps define how the local temporary variables configured for In Maps are assigned to the internal IP-DECT attributes. Out Maps can be configured with the following text fields:

- Dest. Attribute - The name of the IP-DECT attribute. See *IP-DECT attribute name* on page 85 for examples.
- Destination Value - The name of the local temporary variable

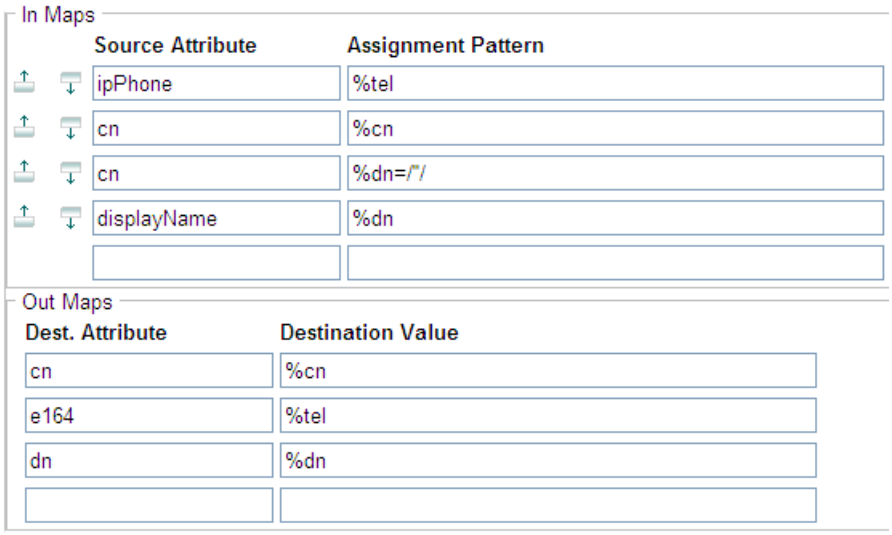
Example



In the example above regular expressions are used to remove non-numerical characters from the phone number (second line of In Maps). The third line of In Maps defines a local temporary variable (dsp) which stores all numbers starting with 031 with "Gbg" added before them. This is shown in the Display attribute as assigned in the Out Maps.

It is recommended to configure a default value for some attributes to avoid the retention of old information in the IP-DECT database. In the example below the display attribute is assigned an empty string if that attribute is not defined in the AD. The Source Attribute in the third line of In Maps is cn because it should be an attribute that is always present in the AD.

Example



Configure AD Server

The IP-DECT system supports only simple binding authentication. However, the default registry setting for Microsoft Active Directory 2003 does not allow simple binds, so it may be necessary to change Windows Registry settings to use AD replication.

1 In Windows, select "Run..." in the Start menu.

2 Enter "regedit" and click "OK" to start the Windows Registry Editor.

3 In the Editor navigate to the "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters\LDAPServerIntegrity" key.

4 Click on the key with the right mouse button and click "Modify".

5 Change the key value of 2 to the value of 1.

6 Click "OK".

8.4.4 Check LDAP Replicator Status

1 Select LDAP > Replicator-Status.

The following information is displayed:

- Server - The IP address and port of the LDAP server.
- Active Directory Replication - Current state of replication. Four states are possible: Stopped, Starting, Up, Down
- Remote - State of replication in the source directory. Three states are possible: Stopped, Active, Completed
- Notify - Number of change notifications received from the server
- Paged - Number of objects received from AD server in response to paged search requests
- No match - Number of objects received that are not matching the configured LDAP filter condition
- Discarded - Number of objects discarded because no suitable map is found
- Local - State of replication in the destination directory. Three states are possible: Stopped, Active, Completed
- Notify - Number of change notifications sent to the server
- Add - Number of locally added objects
- Del - Number of locally deleted objects
- Modify - Number of locally modified objects
- Pending - Number of local objects waiting to be sent to the server

8.4.5 Expert tool

The Expert function should only be used after consultation with Ascom Technical Support.

8.5 DECT

This section describes how to do the following configurations and settings.

- Change System Name and password
- Change Subscription Method
- Configure Authentication Code
- Select Tone system
- Set Default Language
- Set Frequency Band
- Enable/Disable Carriers
- Enable/Disable Local R-Key Handling
- Enable/Disable No Transfer on Hangup
- Configure Coder
- Configure Supplementary Services
- Select Master Mode
- Configure Gatekeeper
- Select Mobility Master mode
- Connect Mobility Master to other Mobility Master(s)
- Enable/Disable Radio
- Enter IP address to the PARI Master and the Standby PARI Master
- Multiple Radio Configuration
- Assign PARI
- Enter SARI
- Configure Air Synchronization

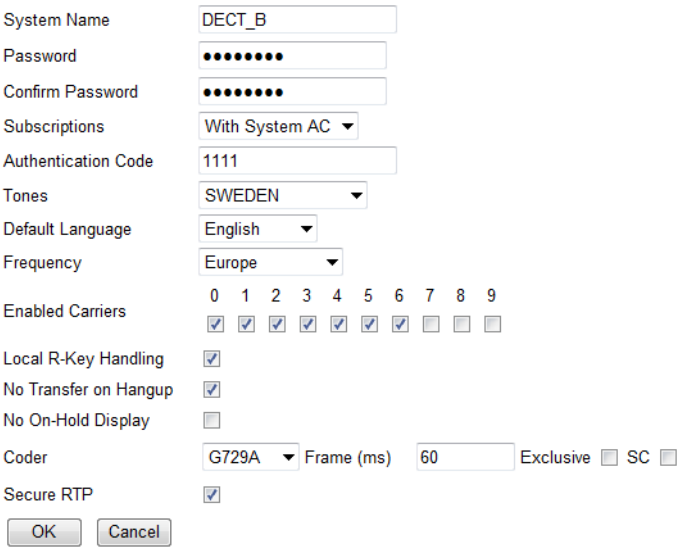


Figure 28. The DECT System configuration page

8.5.1 Change System Name and Password

Note: This is only applicable for a Master, never on a Slave.

The system name and password must be the same for all IPBS/IPBLs throughout the system. Reset in order to make the changes take effect, see 8.22 *Reset* on page 138.

Note: If Ascom VoIP Gateway is the LDAP server, the password in the IPBS/IPBL must be identical to the Ascom VoIP Gateway (PBX/Password).

1 Select DECT > System.

Note: To access the System tab, the Master mode has to be activated, see 8.5.13 *Select Mode* on page 94.

2 Write a system name in the System Name text field.

3 Enter a new password in the Password text field. Repeat the password.

4 Click "OK".

Note: It is recommended to create a backup of the IPBS configuration when the password has been changed, see 8.14 *Backup* on page 126.

8.5.2 Set Subscription Method

The IP-DECT system can be set to use the following subscription methods:

- With User AC - Individual Registration and Auto Registration is possible.
- With System AC - Anonymous Registration and Individual Registration is possible.
- Disable - Registration is not possible.

Select subscription method:

1 Select DECT > System.

Note: To access the System tab, the Master mode has to be activated, see 8.5.13 *Select Mode* on page 94.

2 Select subscription method in the Subscriptions drop-down list.

3 Click "OK".

Note: When"With System AC" is enabled anyone could register to the IP-DECT System.

8.5.3 Configure Authentication Code

If "allow anonymous subscription" method is selected it is needed for the IP-DECT system to have an authentication code configured. The authentication code is generated automatically but can be modified manually by selecting a code consisting of 4 to 8 numbers (0-9).

1 Select DECT > System.

Note: To access the System tab, the Master mode has to be activated, see 8.5.13 *Select Mode* on page 94.

2 Enter an authentication code in the Authentication Code text field.

3 Click "OK".

8.5.4 Select Tones

1 Select DECT > System.

NOTE: To access the System tab, the Master mode has to be activated, see 8.5.13 *Select Mode* on page 94.

2 Choose tones in the Tones drop-down list.

3 Click "OK".

8.5.5 Set Default Language

If the handset does not send language information to the system, this setting determine which language that is displayed for some text messages (for example hung-up and disconnected).

1 Select DECT > System.

Note: To access the System tab, the Master mode has to be activated, see 8.5.13 *Select Mode* on page 94.

2 Choose language in the Default Language drop-down list.

3 Click "OK".

8.5.6 Set Frequency Band

The IPBS/IPBL can operate in the following frequency bands:

- 1880 - 1900 MHz, Europe, Africa, Middle East, Australia, New Zeeland and Asia
- 1910 - 1930 MHz, South America
- 1920 - 1930 MHz, North America

1 Select DECT > System.

NOTE: To access the System tab, the Master mode has to be activated, see 8.5.13 *Select Mode* on page 94.

2 Select frequency area in the Frequency drop-down list.

3 Click "OK".

4 Reset in order to make the changes take effect, see 8.22 *Reset* on page 138.

8.5.7 Enable Carriers

The IPBS/IPBL has 5 carriers for the North American frequency band and 10 carriers for the other frequency bands. Under all normal circumstances all carriers should be enabled.

To enable or disable carriers:

1 Select DECT > System.

NOTE: To access the System tab, the Master mode has to be activated, see 8.5.13 *Select Mode* on page 94.

2 Select/clear the Enabled Carriers check boxes.

3 Click "OK".

8.5.8 Local R-Key Handling

With this option enabled keypad information is handled locally. If this option is disabled keypad information is sent transparently to the IP-PBX. Local R-key handling is further described in *Appendix C*.

1 Select DECT > System.

NOTE: To access the System tab, the Master mode has to be activated, see 8.5.13 *Select Mode* on page 94.

2 To enable, select the Local R-Key Handling check box.
NOTE: To access the Local R-Key Handling check box, the SIP protocol has to be selected on the Master, see 8.5.16 *Configure Gatekeeper* on page 95.

3 Click "OK".

8.5.9 No Transfer on Hangup

If enabled it will not be possible to do a transfer by hanging up the handset. R4 must be pressed (see *Appendix C*).

1 Select DECT > System.

NOTE: To access the System tab, the Master mode has to be activated, see 8.5.13 *Select Mode* on page 94.

2 To enable, select the No Transfer on Hangup check box.

3 Click "OK".

8.5.10 Configure Coder

Select the preferred coder, and enter the desired frame length. If exclusive is selected for the coder the IPBS/IPBL is forced to use that coder. With Silence Compression enabled no information is sent during pauses in the conversation, this is used to save bandwidth.

Note: When exclusive is enabled for a coder it might be impossible to make calls outside the IP-DECT system.

1 Select DECT > System.

Note: To access the System tab, the Master mode has to be activated, see 8.5.13 *Select Mode* on page 94.

2 Choose the applicable coder in the Coder drop-down list.

NOTE: The G726-32 coder is not supported by SIP.

3 Enter the sample time in milliseconds in the Frame text field.

4 Choose Exclusive enabled or disabled by selecting/clearing the Exclusive check box.

5 Choose Silence Compression enabled or disabled by selecting/clearing the SC check box.

6 Click "OK".

8.5.11 Secure RTP

This option makes it possible to encrypt media streams. The encryption is activated if the SRTP is also enabled in the IP-PBX. For additional privacy it is recommended to use the encrypted signalling protocol (SIPS) as well to hide the exchange of the SRTP keys.

Note: If SRTP is enabled one Radio can handle maximum 5 calls for IPBS1 and 40 calls for IPBL (including relayed calls) at the same time. For this reason and because of the high load on the CPU when SRTP is used, it is recommended to deactivate the Radio in the Master.

1 Select DECT > System.

Note: To access the System tab, the Master mode has to be activated, see 8.5.13 *Select Mode* on page 94.

2 To enable SRTP: Select in the Secure RTP drop-down list a cryptographic suite. The numbers in the list refer to key-length/sha1 hash-length.

To disable SRTP: Select in the Secure RTP drop-down list the empty row at top.

3 Click "OK".

If a call is successfully encrypted a lock icon appears next to the ongoing call description in the Traffic > Master Calls section.

8.5.12 Configure Supplementary Services

The supplementary services determine how to handle a call if for example busy or not answered by the user.

1 Select DECT > Suppl. Serv.

NOTE: To access the *Suppl. Serv.* tab, the Master mode has to be activated, see 8.5.13 *Select Mode* on page 94.

2 Select the *Enable Supplementary Services* check box to activate the supplementary services below. The default Activate and Deactivate feature codes are preset.

Note: To disable a specific service, select the Disable check box in front.

Feature	Description
Call Forwarding Unconditional	Forwards incoming calls to a given number in all cases
Call Forwarding Busy	Forwards incoming calls to a given number if the handset is busy

Feature	Description
Call Forwarding No Reply	Forwards incoming calls to a given number if the call is not answered or there is no coverage
Do Not Disturb	Sets the handset in busy mode
Call Waiting	A second incoming call during a call is indicated with a call waiting tone
Call Completion Busy Subscriber	Notifies the caller when a busy number becomes available and reinitiates the call. Only works on H.323
Logout User	Logs out the user and the handset becomes anonymously subscribed.
Clear Local Settings	Clears all locally stored feature settings and all features are deactivated
MWI Mode	MWI (Message Waiting Indication) enables the receiving of a notification from an IP-PBX when, for example, a voice mail is available for listening. There are four modes that can be selected to enable MWI: Fixed interrogate and fixed notify number User dependent interrogate number User dependent notify number Both numbers users dependent "Fixed" means that a common call number is used for all users. "User dependent" means that the user's own call number is used.
MWI Interrogate Number	The number used by the handset when it checks with the IP-PBX if there are any message waiting indications to be notified about.
MWI Notify Number	A call number shown in the handset display when receiving a MWI notification. To receive the stored message the user dial the number.
Local Clear of MWI	If necessary, enter the number of the message center in this field to clear the message waiting indication locally when dialling the number.
External Idle Display	Depending on type of IP-PBX, absence and call forwarding texts will be displayed on the handset when idle. Note: If call forwarding is handled by the IP-PBX, the following options must be disabled: Call Forwarding Unconditional Call Forwarding Busy Call Forwarding No Reply

3 Click "OK".

4 Reset in order to make the changes take effect, see 8.22 *Reset* on page 138.

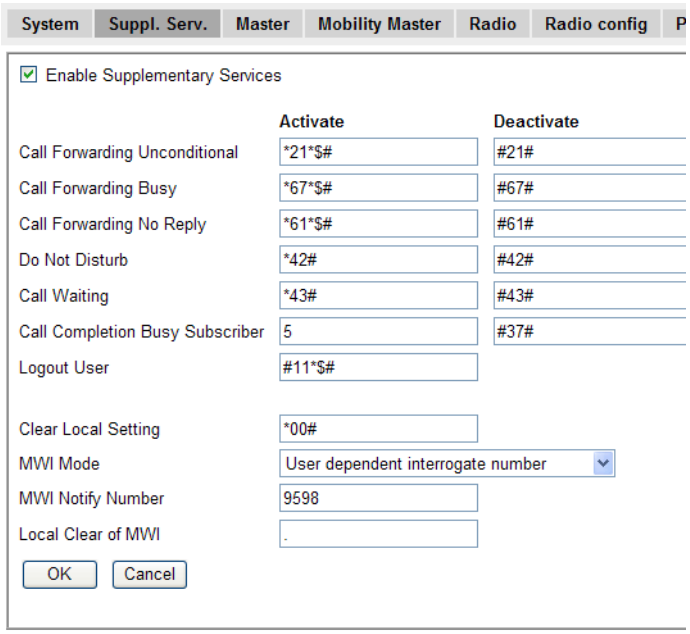


Figure 29. Supplementary services

8.5.13 Select Mode

1 Select DECT > Master.

2 Select in the Mode drop-down list:

- "Off", if this IPBS/IPBL is a Slave
- "Active", if this IPBS/IPBL is the Master.
- "Standby", if this IPBS/IPBL is the Standby Master.
- "Deployment" is used for coverage test only. The speech from the handset is looped back to the handset.

3 If you have selected the "Standby" mode enter the primary Master IP address in its text field.

4 Click "OK".

5 Reset in order to make the changes take effect, see 8.22 *Reset* on page 138.

8.5.14 Set Master Id

1 Select DECT > Master.

2 Enter a Master id in the Master Id field. The id must be unique for each Master in a multiple Master system. The Standby Master must have the same id as the Master.

3 Reset in order to make the changes take effect, see 8.22 *Reset* on page 138.

8.5.15 Enable PARI Function

The PARI Master is responsible for assigning PARIs, being part of the same external handover domain, to the Radios associated. A Radio will always be given the same PARI, based on the PARI-mac-address-association.

1 Select DECT > Master.

2 If this is the Pari Master or standby Pari Master, select the Enable Pari function check box.

Note: Only one Master per handover and sync domain can have the Pari function enabled.

3 Reset in order to make the changes take effect, see 8.22 *Reset* on page 138.

8.5.16 Configure Gatekeeper

The Master need to know the address to the system gatekeeper.

1 Select DECT > Master.

2 Select "H.323", "SIP", "TSIP" or "SIPS" protocol in the *Protocol* drop-down list.

If H323 protocol is selected, continue with step 3 and 4. Otherwise, jump to step 5.

3 Enter the address to the gatekeeper in the *Gatekeeper IP address* text field.

4 Enter the address to the alternative gatekeeper in the *Alt-Gatekeeper IP address* text field.

NOTE: As an alternative to the Gatekeeper IP Address, the Gatekeeper ID can be used.

5 NOTE: Step 5 to 7 applies to the SIP, TSIP or SIPS protocols.

SIP uses the UDP protocol, TSIP uses the TCP protocol, and SIPS uses the TLS protocol.

Enter the IP address or host name and optionally port of proxy (e.g. proxy1.example.com:5060) to the SIP proxy (registrar) in the Proxy text field.

6 Enter the IP address or host name and optionally port of proxy (e.g. proxy2.example.com:5060) to the alternative SIP proxy (registrar) in the *Alt. Proxy* text field.

7 If used, enter the domain address in the *Domain* text field.

8 Enter the maximum internal number length in the *Max. internal number length* text field.

9 To enable "Enbloc Dialing", select the Enbloc Dialing check box.

With this option enabled the keystrokes on the handsets are buffered in the IPBS/IPBL for a short period of time before sent to the IP-PBX (use this when the IP-PBX does not support overlap sending). If disabled the keystrokes are immediately sent to the IP-PBX.

10 To enable "DTMF through RTP Channel", select the DTMF through RTP channel check box.

If enabled DTMF is negotiated according to RFC2833/4733, resulting in DTMF digits being sent as RTP payload directly to the other endpoint. If the other party does not support RFC2833/4733, there will be fallback to DTMF over the signalling channel (SIP INFO or H.245)

If disabled, the DTMF is always sent in the signalling channel.

11 To enable "Short disconnect tone", select the Short disconnect tone check box.

With this option enabled, a short tone (i.e. busy tone) is received when the other party hangs up. If this option is not enabled, busy tones will be received for a longer period of time.

12 If you in step 2 selected "SIP" protocol, enable or disable the following options in the SIP Interoperability Settings section:

Registration time-to-live
This is the Expires-header in the REGISTER message. The default is 120 seconds. To enable this option, enter a value specified in seconds in the "Registration time-to-live" field. Note: Depending on the number of users, the entered value may have to be increased. For example, for 500 users it is recommended to enter 300 seconds and for 1000 users it is recommended to enter 600 seconds. The SIP proxy might respond to the REGISTER with a different value. Then the responded value will be used for REGISTER refresh.
When secondary SIP proxy is in use, for example when the primary SIP proxy is down, the configured time-to-live value is used to decide how often the Master will try to reconnect to the primary SIP proxy.

Hold Signalling
Some IP-PBXs require special way of hold signalling. In the "Hold Signalling" list field, select one of the following:
inactive: No media stream is sent or received.
sendonly: Media stream is sent only and not received.
sendonly with 0.0.0.0: Special case of sendonly where also the media IP address is set to 0.0.0.0.

Hold before Transfer
If this option is enabled, the consultation call is put on hold before transfer. Some IP-PBXs require this option so that both called parties are put on hold before the transfer is carried out.
To enable this option, select the "Hold before Transfer" check box.

Accept Inbound Calls not Routed via Home Proxy
If this option is enabled it could be possible for inbound calls to bypass call restrictions configured in the IP-PBX. If it is disabled a 305 Use Proxy response will be sent.
To enable this option, select the "Accept inbound calls not routed via home proxy" check box.

Register with number
If this option is enabled, number will be used for registrations towards the IP-PBX instead of name. Name will be used for authentication.
To enable this option, select the "Register with number" check box.

KPML support
If this option is enabled, the DTMF digits are sent with the SIP signalling using the Keypad Markup Language (KPML) method.With this method single DTMF digits can also be sent during call setup to add digits to the callend number (overlap sending). Enbloc dialing can then be unchecked. The IP-PBX must also support KPML.
To enable this option, select the KPML support check box.

Make sure that the Allow DTMF through RTP and the Send inband DTMF check boxes are cleared.

13 Click "OK".

14 Reset in order to make the changes take effect, see 8.22 *Reset* on page 138.

If you in step 2 selected the "SIPS" protocol the IPBS downloads a certificate from the IP-PBX to ensure a secure transaction. The IPBS does not initially trust the certificate so it must be added manually to the trust list of the IPBS. It is also possible that more than one certificate is downloaded creating a certificate chain. The root CA certificate is at the end of the chain which contains a self-signed signature and it is able to approve other certificate requests. It is recommended to add the root CA certificate to the IPBS trust list.

Note: The connection to the IP-PBX will only be established after the certificate is acknowledged.

If the certificate expires, the ongoing connection is maintained but it will not be possible to start a new connection until the certificate is renewed.

To add a certificate to the trust list do the following:

1 Select General > Certificates.

2 In the Rejected certificates section select the check box of the certificate you want to trust.

3 Click "Trust".

To ensure two-way authentication the IP-PBX also downloads a certificate from the IPBS. The trust list must also be manually updated with this certificate in the IP-PBX similarly to the IPBS.

For more information about certificate handling, see 8.1.10 *Certificates* on page 73.

8.5.17 Registration for Anonymous Devices

Handsets registered anonymously can make emergency calls through an extension reserved for anonymous users.

Note: Call restrictions must be configured in the PBX to allow for emergency calls only.

This option also provides a solution for the case when the Master, running on an IPBS with local power or an IPBL, loses IP connectivity without the local host Radio losing its connection to the Master. The handsets locked to this Radio become isolated from the system without any notification.

1 Select DECT > Master.

2 Enter the registration name and number to the PBX in the Registration Name / Number text fields.

3 Select the "Deactivate Master if no connection" check box to make the Master deactivate itself if the anonymous registration to the PBX fails. As a result the local host Radio will fail to register to the Master, and handsets, depending on their type, can move to another Radio that is operable.

Note: It is not recommended to use this option for a Master without a Standby Master.

4 Click "OK".

Note: A simpler and reliable way to handle this case is to deactivate the local host Radio on the Master.

8.5.18 Select Mobility Master Mode

In a system with two or more Masters (Multiple Master system), a Mobility Master must be configured. For more information on Multiple Master Systems, see the System Planning documentation for IP-DECT.

1 Select DECT > Mobilty Master.

2 Select in the Mode drop-down list:

- "Active", if this IPBS/IPBL is the Mobility Master.
- "Standby", if this IPBS/IPBL is the Standby Mobility Master.

3 If you have selected the "Standby" mode: Enter the primary Mobility Master IP address in its text field.

4 Write a login name in the Name text field.

5 Enter a password in the Password text field.

6 Click "OK".

8.5.19 Connect Mobilty Master to other Mobility Master(s)

1 Select DECT > Mobilty Master.

2 Write a name in the *Name* text field.

3 Enter a password in the *Password* text field.

4 Enter the address to the other Mobility Master in the *IP Address* text field.

5 Enter the address to the Standby Mobility Master for the other Mobility Master in the *Alt. IP Address* text field.

6 Click "OK".

7 Repeat the above steps to connect to additional Mobility Masters.

8.5.20 Disconnect Mobilty Master from other Mobility Master(s)

1 Select DECT > Mobilty Master.

2 Delete the name in the *Name* text field.

3 Delete the password in the *Password* text field.

4 Delete the address to the other Mobility Master in the *IP Address* text field.

5 Delete the address to the Standby Mobility Master for the other Mobility Master in the *Alt. IP Address* text field.

6 Click "OK".

7 Repeat the above steps to disconnect from additional Mobility Masters.

Note: When disconnecting from other Mobility Master(s) the password field might have to be reentered.

8.5.21 Connect Master to a Mobility Master

In a system with several Masters, all Masters must be connected to the Mobility Master.

1 Select DECT > Master.

2 Enter the name for the Mobility Master in the *Name* text field.

3 Enter the password for the Mobility Master in the *Password* text field.

4 Enter the address to the Mobility Master in the *IP Address* text field.

5 Enter the address to the Standby Mobility Master in the *Alt. IP Address* text field.

6 Click "OK".

7 Reset in order to make the changes take effect, see 8.22 *Reset* on page 138.

8.5.22 Enable the Radio

If the IPBS/IPBL not shall be used as a radio, for example only be used as a *PARI* Master, it can be disabled by marking the *Disable* checkbox.

Tip: To assign a PARI Master, see 8.5.23 *Enter IP Address to the PARI Master and the Standby PARI Master* on page 99.

1 Select DECT > Radio.

2 Clear the *Disable* check box.

8.5.23 Enter IP Address to the PARI Master and the Standby PARI Master

All IPBS/IPBL need to know the IP address of the PARI Master and the Standby PARI Master.

1 Select DECT > Radio.

2 Enter the name for the PARI Master in the *Name* text field.

3 Enter the password for the PARI Master in the *Password* text field.

4 Enter the address to the PARI Master in the *PARI Master IP Address* text field. If this is the PARI Master, enter 127.0.0.1.

5 Enter the address to the Standby PARI Master in the *Standby PARI Master IP Address* text field. If this is the Standby PARI Master, enter 127.0.0.1.

6 Click "OK".

7 Reset in order to make the changes take effect, see 8.22 *Reset* on page 138.

8.5.24 Multiple Radio Configuration

The PARI Master can configure the same Radio settings for all Radios in the system. All settings configured in the *Radio Config* page replace the local Radio settings. This means that all settings in the *Radio Config* menu will have precedence over values configured locally or received via DHCP options.

1 Select DECT > Radio Config.

NOTE: To access the Radio Config. tab, the PARI function has to be enabled, see 8.5.15 *Enable PARI Function* on page 94.

2 Configure alarm and event forwarding, see *Forward Alarms and Events* on page 70.

3 Configure automatic firmware update, see 8.1.4 *Configure Automatic Firmware Update* on page 68.

4 Configure NTP settings, see 8.1.5 *Configure the NTP Settings* on page 68.

5 Configure IP settings, see 8.3.1 *Configure IP Settings* on page 81.

6 Click "OK".

8.5.25 PARI

The PARI is a part of the broadcast identity, which uniquely identifies an IPBS/IPBL. This PARI is automatically assigned to each IPBS/IPBL in the system. But if more than one Ascom IP-DECT system operates within the same coverage area, the systems need to have a unique system identity in the PARI assigned in order to differentiate the systems.

To see the occupied system IDs of other Ascom IP-DECT systems within the coverage area, perform an RFP scan, see 8.21.10 *RFP Scan* on page 137.

1 Select DECT > PARI.

NOTE: To access the PARI tab, the PARI function has to be enabled, see 8.5.15 *Enable PARI Function* on page 94.

2 Select a number between 1 and 292. If this is not done, the IPBS/IPBL will randomly select a number.

NOTE: The number of system IDs will affect how many IPBSs/IPBLs that can be used per PARI Master in an installation, as shown below:

System ID = 1 to 36: Max. 1023 IPBS / Pari Master
Max. 240 IPBL / Pari Master

System ID = 37 to 292: Max. 127 IPBS / Pari Master
Max. 127 IPBL / Pari Master

3 Click "OK".

4 Reset in order to make the changes take effect, see 8.22 *Reset* on page 138.

Note: The RFPI, which the PARI is a part of, can be used for localization of a handset making a personal alarm. To ensure that RFPIs are system unique, use different System ID's for each PARI Master.

8.5.26 SARI

The SARI is the broadcast identity, which uniquely identifies an IP-DECT system. The SARI is added in the PARI Master. It is possible to add more than one SARI (guest SARIs). This is necessary if you want to join two separate IP-DECT systems and allow handsets to roam into each other's system. The advantage is that the handsets in the two different IP-DECT systems need not be re-registered to a common SARI.

Note: Several guest SARIs have an impact on the system performance, so it is recommended to use the same SARI across all PARI Masters in the system. If this is not feasible, you can add up to 10 SARIs.

1 Select DECT > SARI.

Note: To access the SARI tab, the PARI function has to be enabled, see 8.5.15 *Enable PARI Function* on page 94.

2 Enter the SARI number in the SARI text field.

3 Click "OK".

4 You can add optional guest SARI numbers in the empty field.

5 Click "OK". All RFPs are reinitialized to broadcast also the added guest SARI.

8.5.27 Configure Air Synchronization

This section only applies to the IPBS.

IPBS System

The IPBSs use the DECT air interface to synchronize to each other. For an individual IPBS it is not needed to configure which IPBS to synchronize to. It is needed to manually select one or several IPBS as synchronization master candidate. The PARI Master assigns one of these IPBS as an active sync master. The remaining candidates will act as sync slaves and can be new sync masters in case the active sync master will fail/break. When using one sync region it is recommended to configure at least two base stations in the middle of the building as synchronization masters.
All IPBSs in sync slave mode sends its list over received sync candidates to the PARI Master. The PARI Master informs the IPBS sync slaves which sync candidate it shall synchronize to.

Mixed System

All IPBLs are synchronization masters in region 0. Any IPBS in this region will receive its synchronization over the air from the RFPs, which are connected to the IPBL.

Sync Regions

Sync regions are used when, for example, several buildings are located in the same coverage area and all radios are using same PARI Master but where the synchronization coverage between buildings is not good enough for a stable synchronization.

A solution may be to use separate synchronization regions for the buildings and have reference synchronization between the regions. Each region has its own Sync Master but can take reference sync from another region and handover between the buildings is possible. If a region should lose the reference synchronization with another region, the internal synchronization in respective region will still work but there can be no handover between the regions.

Note: For the synchronization to work, it is not allowed to configure reference sync in a ring.

Configure Sync Slave IPBS

All IPBSs in sync slave mode sends its list of sync candidates to the PARI Master. The PARI Masters informs the IPBS sync slave which sync candidate it shall synchronize to.

In addition to the above automatic synchronization procedure it is also possible to use static synchronization, that is, manually lock on to a specific RFPI. When specifying a specific RFPI, it must be within the same synchronization region.

Configure Sync Slave as follows:

1 Select DECT > Air Sync.

2 Select "Slave" in the *Sync Mode* drop-down list.

3 To lock the sync slave to a specific RFPI, enter the sync RFPI in the *Sync RFPI* text field. Enter an alternative sync RFPI in the *Alternative Sync RFPI* text field (optional).

4 Enter a region ID between 0 and 63 in the *Sync Region* text field.

5 Click "OK".

Configure Sync Master IPBS

Radios configured as sync master will report to the PARI Master that it wants to be a sync master. The PARI Master will select one of them to be the active sync master.

When a sync master has been assigned to be active it searches for other IPBSs within the same region during 30 seconds. If any IPBS is found the values for slot, frame, multi frame and PSCN are received and applied to the Sync Master. After receiving all these values or after the time-out of 30 seconds the Sync Master enters the master state.

With this method it will be possible to restart only the Master in the region. The remaining slaves will be able to maintain synchronization for a few minutes during restart of the Master. The Master will adjust itself to the other IPBSs at startup. The slaves will notice that the Master is back and the synchronization will be received from the Master.

In master state the values are updated locally during all further operation of the Master IPBS and no synchronization to other IPBSs in the same region is done.

It is possible to configure the Sync Master to synchronize to a reference base station (another or same DECT system). In this case the Sync Master will try to synchronize to the reference system if the reference system is found but it will not require the reference system to be available. The Sync Master will operate even though the reference system is not available. During startup the Master will prefer to synchronize to a slave base in the same system before synchronizing to the reference base station.

Configure Sync Master as follows:

1 Select DECT > Air Sync.

2 Select "Master" in the *Sync Mode* drop-down list.

3 To synchronize the sync master to a reference base station, enter the reference base station in the *Reference RFPI* text field. Enter an alternative reference base station in the *Alternative reference RFPI* text field (optional).

4 Enter a region ID between 0 and 63 in the *Sync Region* text field.

5 Select type of resynchronization action to perform at reference sync failure, a manual or an automatic (scheduled) one.

6 Click "OK".

8.6 VoIP

This section only applies if the SIP protocol is used in the system.

8.6.1 Add instance id to the user registration with the IP-PBX

This might simplify administration with some IP-PBXs.

1 Select VoIP > SIP.

2 To enable, select the "Add instance id to the user registration with the IP-PBX" check box corresponding to the SIP protocol that is used.

3 Click "OK".

8.6.2 IP-PBX supports redirection of registration when registered to alternative proxy

When the primary proxy is down and an alternative proxy is in use, the IP-PBX will redirect the registration to the primary proxy when available again. IP-DECT will not make any attempts to contact the primary proxy as long as the alternative proxy is available.

1 Select VoIP > SIP.

2 To enable, select the "IP-PBX supports redirection of registration when registered to alternative proxy" check box corresponding to the SIP protocol that is used.

3 Click "OK".

8.6.3 Use local contact port as source port for TCP/TLS connections

Instead of having a dynamic/ephemeral source port for the persistent TCP/TLS connection, the local contact port of the corresponding phone can be used instead (required by some IP-PBXs.).

1 Select VoIP > SIP.

2 Select the *SIPS* check box.

3 Click "OK".

8.6.4 Session Timer (initial value)

If set, a keep-alive mechanism will be used to detect if a call is still valid as defined by rfc 4028. This is normally handled by the IP-PBX and then not necessary to be defined here.

1 Select VoIP > SIP.

2 To enable, enter a time (sec.) in the "(Session Timer initial value)" field.

3 Click "OK".

8.7 UNITE

8.7.1 Configure Messaging

Note: The Unite CM support for the below functions is depending on the Unite CM software version.

If an IMS3/Unite CM is to be used in the IP-DECT system, enter the IP address following the steps below.

1 Select UNITE > SMS.

NOTE: To access the SMS tab, the Master mode has to be activated, see 8.5.13 *Select Mode* on page 94.

2 Enter the address to the IMS3/Unite CM in the IP Address text field.

3 Click "OK".

If Multicast is to be used, do as follows:

1 Select UNITE > SMS.

NOTE: To access the SMS tab, the Master mode has to be activated, see 8.5.13 *Select Mode* on page 94.

2 Select the Multicast checkbox.

NOTES:
a) The Multicast groups are created in the ESS, refer to Installation and Operation Manual, Enhanced System Services, TD 92253GB.
b) In a Multiple Master System all users to be reached by a Multicast message must be assigned to the PARI Master.
c) In order to support Multicast messaging the IMS3 must be installed with version 2.62 or later
d) To support multicast only Worf (KRCNB 30x , BS3x0 and DB1) RFPs shall be used.

3 Click "OK".

If the communication between the Master and the IMS3/Unite CM should be encrypted, do as follows:

1 Select UNITE > SMS.

Note: To access the SMS tab, the Master mode has to be activated, see 8.5.13 *Select Mode* on page 94.

2 Select the Encryption check box.

NOTES: a) When selecting or clearing the Encryption check box, it may take up to a couple of minutes until the IMS3/Unite CM is fully operational..

b) The IMS3/Unite CM support for encryption is depending on the IMS3/Unite CM software version.

3 Click "OK".

8.7.2 Device Management

If a specific Device Manager (for example IMS3) is to be used in the IP-DECT system, enter the IP address to the Device Manager following the steps below. To set the Master to search for an existing Device Manager on the network, go to 8.7.3 *Service Discovery* on page 104.

1 Select UNITE > Device Management.

NOTE: To access the *Device Management* tab, the Master mode has to be activated, see 8.5.13 *Select Mode* on page 94.

2 Enter the address to the Device Manager in the *Unite IP Address* text field.

The IP address for the Device Manager that the Master is currently connected to is shown under *Active Settings*.

3 Click "OK".

8.7.3 Service Discovery

If no Device Manager (for example IMS3) has been selected to be used in the IP-DECT system, see 8.7.2 *Device Management* on page 104, then the Master will automatically search for an existing Device Manager on the network. To set the Master to search in a specific domain on the network or to stop the search, follow the steps below.

1 Select UNITE > Service Discovery.

NOTE: To access the *Service Discovery* tab, the Master mode has to be activated, see 8.5.13 *Select Mode* on page 94.

2 Do one of the following:

- To stop the Master to search for a Device Manager, select the *Disable* check box.
- To set the Master to search for a Device Manager in a specific domain on the network, enter the domain id in the *Domain ID* text field. The domain id must be the same as the one entered in the Device Manager.

3 Click "OK".

8.7.4 Send Status Log

It is possible to send alarm and event reports to the Unite system. For example directly to the ESS fault handler or to the UNA (Unite Node Assistant) which in turn forwards the alarm event according to distribution lists.

1 Select UNITE > Status Log.

2 Enter the address to the server where the Status Log should be sent in the *Unite IP Address* text field.

3 Enter the Resource Identity/Service in the *Unite Resource Identity* text field. If this field is left empty then the default will be UNA (Unite Node Assistant).

8.7.5 Module Fault List

It is possible to change the severity level on alarms and events generated in the IP-DECT system.

1 Select UNITE > Module Fault List. A list of alarms and events generated in the IP-DECT system is shown with their fault codes (IP-DECT code and Unite code). Alarms are listed with a *Yes* and events are listed with a *No* in the column *Persistant*.

2 To change the severity level on an alarm/event: Select in the *Seriousness* drop-down list one of the following:

- *Disabled* (The alarm/event will not be sent to the Unite system.)
- *Information*
- *Warning*
- *Error*
- *Critical*

3 Click "OK".

Except for severity level *Disabled*, the alarm/event will be sent to the Unite system with changed severity level.

8.8 Import and Export a Central Phonebook

Note: If the phonebook functionality in the IPBS/IPBL is enabled, then the SMS feature in the IMS3/Unite CM is disabled. If an IMS3/Unite CM is connected, the central phonebook should be located in the IMS3/Unite CM instead of the IPBS/IPBL.

Import Entries to the Central Phonebook from a csv file

Note: A csv file can contain max 1000 users.

The csv file to be imported to the phonebook shall have the following format:

```
First name 1;Last name 1;Telephone number 1
First name 2;Last name 2;Telephone number 2
```

or

```
First name 1,Last name 1,Telephone number 1
First name 2,Last name 2,Telephone number 2
```

Note: When importing a central phonebook file in csv format, existing entries are deleted.

1 Select "Central Phonebook".

2 Select the *Enable* check box.

3 Select file type for the csv file in the *File Type* drop-down list.

4 If so needed, select separator for the csv file in the *Delimeter* drop-down list.

5 Click "OK". The options *Import* and *Export* are displayed.

6 Select Import > Choose File.

7 Locate the csv file in the system and select Open > Next. Make sure the correct number of entries are correct.

8 Click "Close"

Export the Central Phonebook to a csv file

The complete phonebook can be exported to a csv file for example for editing or backup reasons.

1 Select "Central Phonebook".
2 Click "Export".
3 Click "Download file" in the window that appears.
4 Click "Save" in the dialog window that appears.
5 Enter a name of the file and select in which folder the file should be saved.
6 Click "Save".

8.9 Users

This section describes the *Users* sub menu and how to do the following:

- Show all registered users in the IP-DECT system.
- Search for user information.
- Add a user.
- Add a user administrator.
- Import a csv file with user information.
- Export a csv file with user information.

8.9.1 Show all Registered Users in the IP-DECT System

Shows both User Administrator and Users.

1 Select Users > Users.
2 Click "show".

It is possible to change the order of the list by clicking on the headings.

8.9.2 Search for User Information

It is possible to search for users registered in the system by name or extension number. Search for a user following the steps below:

1 Select Users > Users.
2 Enter the name or number to search for in the text field. It is possible to enter only the beginning of the name or number.
3 Click "show".

8.9.3 Add a User

For information on how to add Users to the IP-DECT system, see 7.13 *Add Users* on page 55.

For information on how to add Administrator to the IP-DECT system, see *Managing User Administrators* on page 49.

8.9.4 Import Users from a csv file

For information on how to add users with Import a csv file to the IP-DECT system, see 7.13.3 *Easy Registration* on page 58.

8.9.5 Export the Users to a csv file

The Users can be exported to a csv file, for example for editing or backup reasons.

1 Click "Export".

2 Click "Save" in the dialog window that appears.

3 Enter a name of the file and select in which folder the file should be saved.

4 Click "Save".

Note: For safety reasons, the *Auth. Code* and *Password* will not be included in the csv file.

8.9.6 Show Anonymous

The IPEI / IPDI number is displayed on anonymous registered handsets.

1 Select "Users".

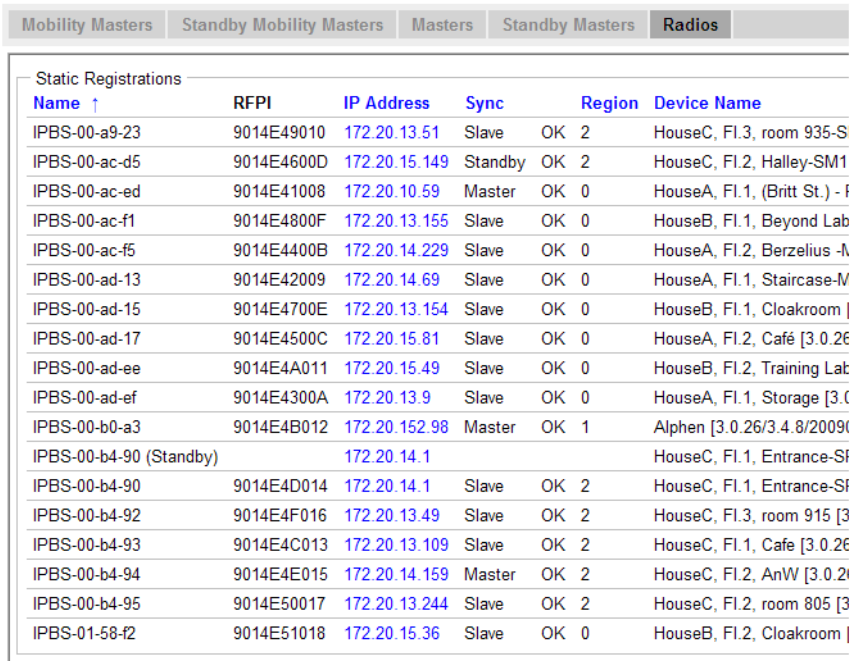
2 Select "Anonymous".

8.10 Device Overview

8.10.1 Radios

Information about the devices in the IP-DECT system.

1 Select Device Overview > Radios.



Name ↑	RFPI	IP Address	Sync		Region	Device Name
IPBS-00-a9-23	9014E49010	172.20.13.51	Slave	OK	2	HouseC, Fl.3, room 935-S
IPBS-00-ac-d5	9014E4600D	172.20.15.149	Standby	OK	2	HouseC, Fl.2, Halley-SM1
IPBS-00-ac-ed	9014E41008	172.20.10.59	Master	OK	0	HouseA, Fl.1, (Britt St.) -
IPBS-00-ac-f1	9014E4800F	172.20.13.155	Slave	OK	0	HouseB, Fl.1, Beyond Lab
IPBS-00-ac-f5	9014E4400B	172.20.14.229	Slave	OK	0	HouseA, Fl.2, Berzelius -M
IPBS-00-ad-13	9014E42009	172.20.14.69	Slave	OK	0	HouseA, Fl.1, Staircase-M
IPBS-00-ad-15	9014E4700E	172.20.13.154	Slave	OK	0	HouseB, Fl.1, Cloakroom
IPBS-00-ad-17	9014E4500C	172.20.15.81	Slave	OK	0	HouseA, Fl.2, Café [3.0.26
IPBS-00-ad-ee	9014E4A011	172.20.15.49	Slave	OK	0	HouseB, Fl.2, Training Lab
IPBS-00-ad-ef	9014E4300A	172.20.13.9	Slave	OK	0	HouseA, Fl.1, Storage [3.(
IPBS-00-b0-a3	9014E4B012	172.20.152.98	Master	OK	1	Alphen [3.0.26/3.4.8/2009(
IPBS-00-b4-90 (Standby)		172.20.14.1				HouseC, Fl.1, Entrance-SI
IPBS-00-b4-90	9014E4D014	172.20.14.1	Slave	OK	2	HouseC, Fl.1, Entrance-SI
IPBS-00-b4-92	9014E4F016	172.20.13.49	Slave	OK	2	HouseC, Fl.3, room 915 [3
IPBS-00-b4-93	9014E4C013	172.20.13.109	Slave	OK	2	HouseC, Fl.1, Cafe [3.0.26
IPBS-00-b4-94	9014E4E015	172.20.14.159	Master	OK	2	HouseC, Fl.2, AnW [3.0.2(
IPBS-00-b4-95	9014E50017	172.20.13.244	Slave	OK	2	HouseC, Fl.2, room 805 [3
IPBS-01-58-f2	9014E51018	172.20.15.36	Slave	OK	0	HouseB, Fl.2, Cloakroom

Name	The unique identification name. The name syntax is ipbs-xx-xx-xx (or ipbl-xx-xx-xx), where xx-xx-xx should be replaced with the last 6 hexadecimal digits of the MAC address.
RFPI	Radio Fixed Part Identity.

IP Address	The IP address, click on the IP address to access the configuration GUI of that IPBS/IPBL.
Sync	The current synchronization status. Should be "Master OK", "Slave OK" or "Standby OK" if synchronized. "Standby" is a Radio configured as a Sync Master but it is active.
Region	The sync region which the Radio belongs to.
Device Name	The name entered in the general menu.
LDAP	The LDAP status, can be "" (blank), "-", "up", "server" or "down". Should be "-", "up" or "server".
Version	The current software version.
Connected Time	The elapsed time since connected to the Master.

Add Radios

In the *Uninitalized Registrations* section, uninitialized Radios not registered to a PARI Master are shown.

1 Select Device Overview > Radios

2 Click "Add" to add the Radio to the Master.

3 In the *Add Radio* window enter a name for the device. You can also add a Standby Master IP Address and a Sync Region.

4 Click "OK".

5 The Radio restarts and it establishes a connection to the PARI Master only.

Delete Radios

In the *Static Registrations* section, initialized Radios no longer registered to the PARI Master are shown.

1 Select Device Overview > Radios

2 In the *Static Registrations* section, click "Delete" to delete the Radio.

The Radio's RFPI is now released and can be reused. All other RFPIs in use are not affected.

Move RFPIs

In the *Static Registrations* section, initialized Radios no longer registered to the PARI Master are shown. If it is vital that the new device keeps the RFPI for the broken device e.g. alarm localization purposes, move the RFPI for the broken device to the new device registered to the PARI Master.

1 Connect the replacing device.

2 Add the Radio to the PARI Master, see *Add Radios* on page 108.

3 Select Device Overview > Radios

4 In the *Static Registrations* section, click "Move" for the Radio that is broken.

5 In the Move RFPI window, select in the *Destination* section the new Radio that you want to move the broken Radio's RFPI to.

6 Click "Move".

Existing RFPI on the new Radio is replaced by the broken Radio's RFPI. The new Radio's RFPI is now released and can be reused. All other RFPIs in use are not affected. The broken Radio will be deleted from the Static Registrations section.

8.10.2 RFPs

This section only applies to the IPBL.

Information about the DECT devices connected to the IPBL. For explanation on the information, see the table below.

1 Select Device Overview > RFPs.

2 Click the applicable port to open the RFP details pop-up window.

Port	The port used in the IPBL.
Status	Current status of the IPBS connected to the IPBL.
Description	A short description to help identify the IPBS.
RFPI	Identity number.
SW Version	The current software version.
Hardware	The hardware version.
Boot	RFP boot version.
Connected Time	The elapsed time since the RFP connected to the IPBL.
Cable Delay	The delay caused by the cable.
Tx Error	The number of transmitting errors.
Rx Error	The number of receiving errors.

3 The following actions are available:

- Click "OK" to save your settings and close the pop-up window.
- Click "Cancel" to close the pop-up window.
- Click "Refresh" to update the information.
- Click "Reset" to reset the RFP.

8.10.3 Sync Ring

This section only applies to the IPBL.

A wire map of the synchronization ring is available in the GUI. The identities (IPBL-xx-xx-xx) of the IPBLs and the position in the ring is displayed. If the ring is broken it is possible to locate where. Click the IP address to access another IPBL.

1 Select DECT Sync > Sync Ring.

8.10.4 Sync Ports

This section only applies to the IPBL.

Displays the current status of the synchronization ports.

1 Select DECT Sync > Sync Ports.

Status	The current status of the port.

Sync Offset	The synchronization offset for the IPBL.
Cable Delay	The delay caused by the cable.
Sync Lost Counter	The number of times synchronization lost.
Communication	The present status of communication.
Connected to	The IP address of the IPBL connected.
Tx Error	The number of transmitting errors.
Rx Error	The number of receiving errors

8.10.5 Air Sync

This section only applies to the IPBS.

Air Sync status is displayed in the Device Overview > Air Sync menu. For explanation on the information shown for the active and the alternative sync bearers, see the table below.

RFPI	Radio Fixed Part Identity is the Id number of the sync bearer.
Carrier	The carrier used for air synchronization
Slot	The slot used for air synchronization
Hop	The number of hops from the Sync Master to the sync bearer
RSSI	Received Signal Strength Indication
FER	Frame Error Rate, a value between 0 and 100%. Should be below 80% to be able to keep the synchronization.

8.10.6 Sync Lost Counter in IPBS

This section will describe briefly the different situations when the "sync lost counter" is incremented and what impact it has for the users.

Sync Lost Counter

When an IPBS increments the sync lost counter it means that the IPBS stops to handle all radio traffic for a while and after that restarts the synchronization procedure. The radio part is not really restarted but out of service for a short time period. The IP-part of the IPBS is not affected by this but is in service all the time.

There are five reasons for when the sync lost counter is incremented:

- The IPBS has not been able to find a synchronization source within 9 minutes.
- The PSCN value is changed.
- The value for frame number is changed.
- The value for multi frame number is changed.
- The number of enabled carriers is changed.

If the PSCN, frame number, multi frame number and/or the number of enabled carriers is changed, then the radio stops to handle traffic immediately.

Impact for the Users

During speech

If the radio stops to handle traffic as described in *Sync Lost Counter* on page 110, it does not necessarily mean a disconnected call. In a system with good overlapping coverage it might be possible to make a handover to another IPBS without disconnecting the call. If the handset does not quickly find any other IPBS the call will be disconnected and the handset will indicate "No System". As soon as the IPBS is synchronized it is available again for handset communication. The handset will then connect to the system in the same way as for a normal power on.

In idle mode

In idle mode the user will most likely not discover any problem. Since the handsets have a short delay before showing "No System" the handset has time to roam to another IPBS. This requires a good overlap between radio cells to make it possible for the handset to roam to another IPBS. If no other IPBS is available the handset(s) will indicate "No System". As soon as the IPBS is synchronized it is available again for handset communication. The handset will then connect to the system in the same way as for a normal power on.

8.11 DECT Sync

8.11.1 Air Sync Overview

This section only applies to the PARI Master.

To see a graphic presentation of the air synchronization in a system, select DECT Sync > Air Sync Overview.

The internal synchronization for each region is shown separately by an expandable tree view, see Figure 30. The green, yellow and red dots in the sync tree show the following sync status for the Radios:

- Green: Synchronized
- Yellow: Synchronized but poor received signal strength (RSSI < -83 dBm)
- Red: Unsynchronized

The grey dot at top in the sync tree shows that it is a reference sync RFPI.

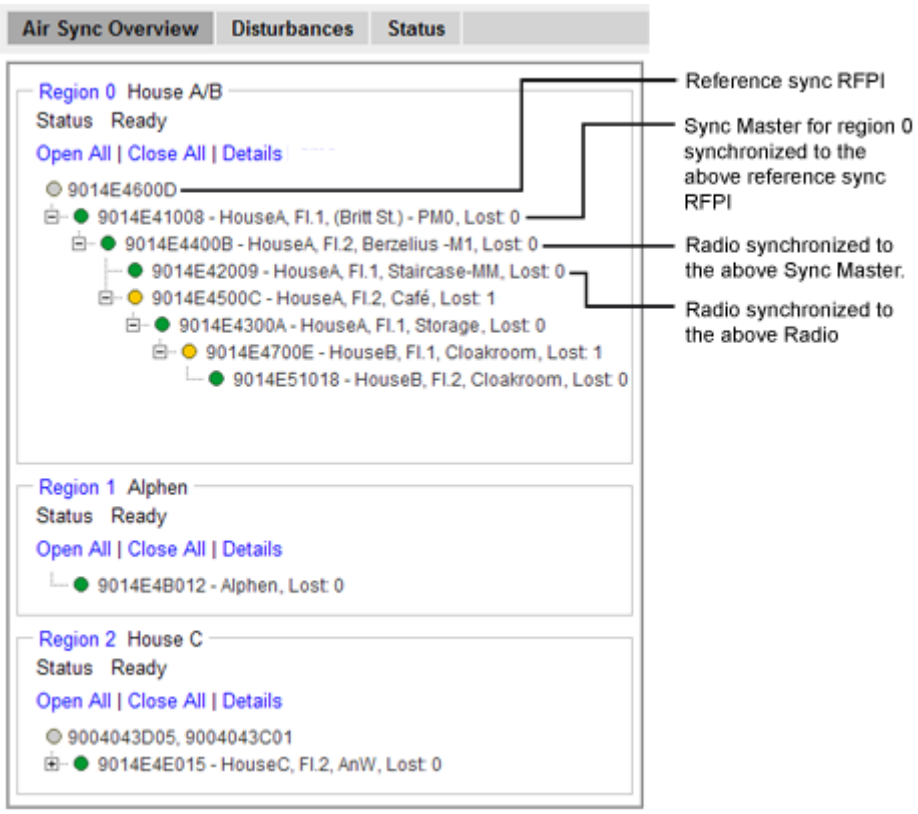

Air Sync Overview
Disturbances
Status
Region 0 House A/B
Status Ready
Open All | Close All | Details
9014E4600D
9014E41008 - HouseA, Fl.1, (Britt St.) - PM0, Lost: 0
9014E4400B - HouseA, Fl.2, Berzelius -M1, Lost: 0
9014E42009 - HouseA, Fl.1, Staircase-MM, Lost: 0
9014E4500C - HouseA, Fl.2, Café, Lost: 1
9014E4300A - HouseA, Fl.1, Storage, Lost: 0
9014E4700E - HouseB, Fl.1, Cloakroom, Lost: 1
9014E51018 - HouseB, Fl.2, Cloakroom, Lost: 0
Region 1 Alphen
Status Ready
Open All | Close All | Details
9014E4B012 - Alphen, Lost: 0
Region 2 House C
Status Ready
Open All | Close All | Details
9004043D05, 9004043C01
9014E4E015 - HouseC, Fl.2, AnW, Lost: 0
Reference sync RFPI
Sync Master for region 0 synchronized to the above reference sync RFPI
Radio synchronized to the above Sync Master.
Radio synchronized to the above Radio

Figure 30. The sync trees for region 0, 1 and 2 where region 0 is fully expanded.

Region Details

1 Select DECT Sync > Air Sync Overview.

2 Click on the region ID text at top above the sync tree.

3 If this has not already been done: In the Region Details window, enter a name for the region.

4 In section Statistics, there are three counters:
- Calculations: Is incremented each time the sync tree is calculated.
- Configurations: Is incremented when an IPBS has received a new sync instruction.
- *Sync Lost*: Is incremented when an IPBS stops to handle radio traffic for a while and after that restarts the synchronization procedure.
To clear the counters, click "Clear".

Reference Synchronization

To get the Sync Master to resynchronize to the reference sync, do as follows:

1 Select DECT Sync > Air Sync Overview.

2 Click on the region ID text at top above the sync tree.

3 In the Region Details window, click "Start". When resynchronizing, all ongoing calls in the region will be disconnected.

IPBS Details

1 Select DECT Sync > Air Sync Overview.

2 Click on the "Details" text link above the sync tree. The sync tree will now display name and sync lost counter for the IPBSs in the region. The sync lost counter is a counter that is incremented when the IPBS stops to handle radio traffic for a while and after that restarts the synchronization procedure.

8.11.2 Disturbances

This section only applies to the PARI Master.

1 Select DECT Sync > Disturbances.

2 Click "Start".

A list of potential disturbances is shown, that is, alien DECT systems that have a higher signal strength than the current sync signal.

8.11.3 Status

This section only applies to the IPBS.

Air Sync status is displayed in the DECT Sync > Status menu. For explanation on the information shown for the active and the alternative sync bearers, see the table below.

Sync offset	Adjustment of frequency in progress performed by the current IPBS so it can be in synchronization with the synch source.
Drift	The time difference between the current IPBS and its sync source.
Sync lost counter	A counter that is incremented when the IPBS stops to handle radio traffic for a while and after that restarts the synchronization procedure.
RFPI	Radio Fixed Part Identity is the Id number of the sync bearer.
Carrier	The carrier used for air synchronization
Slot	The slot used for air synchronization
Hop	The number of hops from the Sync Master to the sync bearer
RSSI	Received Signal Strength Indication
FER	Frame Error Rate, a value between 0 and 100%. Should be below 90% to be able to keep the synchronization.

8.12 Traffic

Traffic information is displayed in the Traffic sub menu. For the Master the traffic information for the IP-DECT system is displayed as well as traffic information for the Radio itself (if this Radio is enabled).

8.12.1 Display All Ongoing Calls in the System

All ongoing calls in the IP-DECT system can be displayed by selecting Traffic > Master Calls in the Master. See the table below for information about the different statistics fields.

Master	
Calls In	The number of incoming calls to the Master.

Calls In Delivered	The number of connected incoming calls in the Master.
Calls Out	The number of outgoing calls in the Master.
Handover	The number of handovers in the Master.
Handover Canceled	The number of failed handovers in the Master.
Abnormal Call Release	The number of abnormal call terminations.
Busy Hour Call Attempts	The number of busy hour calls.
Busiest hour start time	The start time of the busiest hour.

8.12.2 Display Calls

All calls on an IPBS/IPBL can be displayed by selecting Traffic > Radio Calls. See the table below for information about the different statistics fields.

Radio	
Calls In	The number of incoming calls to the Radio.
Calls Out	The number of outgoing calls from the Radio.
Handover	The number of handovers in the Radio.
Handover Canceled	The number of failed handovers in the Radio. NOTE: There can be several reasons for uncompleted handovers occuring. This will in most cases not cause dropped or disconnected calls.

8.12.3 Handover

During call, all ongoing handovers in the IP-DECT system can be displayed by selecting Traffic > Handover in the Master.

8.13 Gateway

IPBS/IPBL has the option to act as a SIP registrar. In fact IP-DECT has several gateway interfaces that independently from each other can handle device registrations.

The gateway functionality is mainly intended for FXO operation (for more information on FXO in IP-DECT see the *Configuration Manual FXO in Ascom IP-DECT System*, *TD 92529GB*) but other uses are possible. Gateways can be used to register to another device such as a gatekepper in a PBX.

SIP interfaces can be used to obtain, for example, a trunk line from a SIP Provider. This solution still requires handset VoIP registrations to be managed in IP-DECT - this is not performed by the SIP provider.

8.13.1 General

1 Select Gateway > General.

2 Select/Enter following settings.

Field name **Description**

- Gatekeeper ID — The Gatekeeper Identifier.
  This is used with VOIP interfaces (GWn) configured as "Gatekeeper/Registrar" as Gatekeeper Identifier (H.323) or Registrar Name (SIP), see 8.13.4 *Gatekeeper Interfaces* on page 119.
  If multiple gatekeepers are installed in a network this can be used to find the right gatekeeper using Gatekeeper Discovery.
  If a PBX is enabled on the same system a different Gatekeeper Identifier must be used for Gateway and PBX.

3 Click "OK".

8.13.2 Interfaces

Select Gateway > Interfaces.

This page shows the gateway's interfaces organized into columns. The individual columns are explained in the table below.

Column	Values	Description
Interface		The descriptive name of the interface. Click this name to open a page, on which all settings can be configured. For more information, see *TEST Interface* on page 115.
CGPN In, CDPN In, CGPN Out, CDPN Out		CGPN In, CDPN In, CGPN Out and CDPN Out mappings. Click the "+" sign next to the interface name to bring up mapping details. For more information see *Call Number (CGPN/CDPN) Mappings* on page 118.
State		The current state of the interface at protocol level. Possible states are: Up, Down.
Alias		The H.323 call name and the E.164 call number.
Registration		If a terminal has successfully registered with an SIP or TEST interface, then this is indicated in this column through specification of the IP address <Name of the interface:Call number:IP address>.

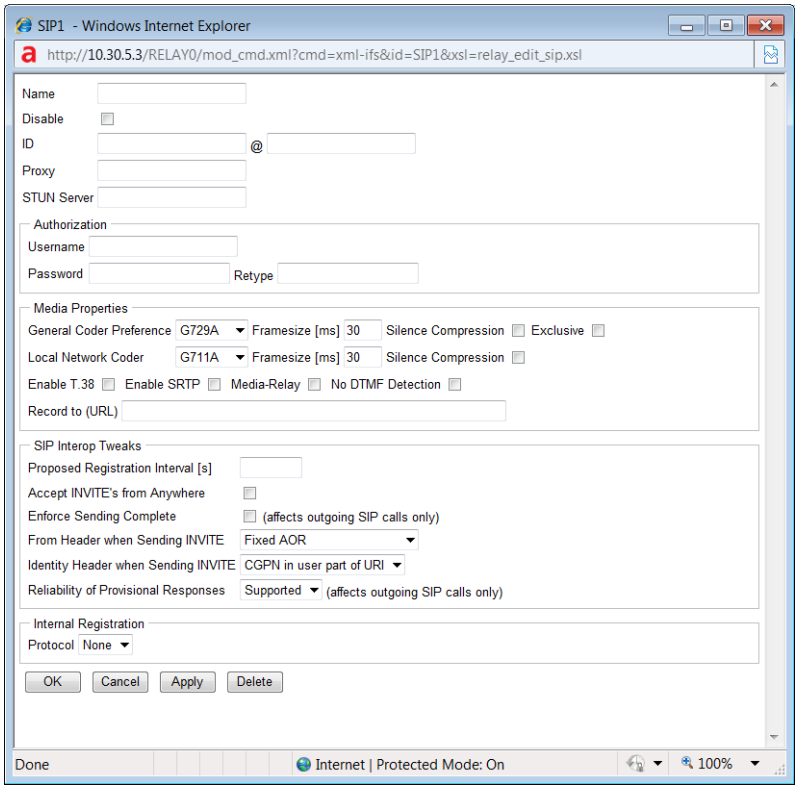
TEST Interface

Normally there is one non-configurable, internal TEST interface called TEST, usable only as the destination for a call. If a call is received on this interface, the on hold music stored in the non-volatile memory is played. Incoming calls must be in G.729A or G.723 format; other formats are not supported. Suffix dialling digits are ignored.

8.13.3 SIP Interfaces

1 Select Gateway > SIP.

2 Click on one of the SIP interfaces (SIP1 - SIP4) under the *Interface* heading. A new window opens.



3 Select/Enter following settings:

Field name	Description
• Name	Enter a name for the SIP interface
• Disable	Select the Disable check box to disable the Interface
• ID	Enter the registration ID followed by the SIP provider domain name preceded by an @ (for example 8111111e0@sipgate.de).
• Proxy	The IP address of the SIP provider to where the SIP messages (REGISTER,INVITE,etc.) are to be sent.
• STUN Server	Only necessary if the SIP server is outside the private network. Note: STUN Server has not been tested and is not officially supported by the Ascom IP-DECT System.
Authorization	
• Username	Username for authorization (only if different from the registration ID).
• Password / Retype	The password for authorization must be specified here (Password) and confirmed (Retype).
Media Properties	
• General Coder Preference	Select the applicable coder in the drop-down list.
• Framesize	Enter the sample time in milliseconds.

• Silence Compression	Select this check box to enable silence compression.
• Exclusive	Select this check box to accept only preset coders.
• Local Network Coder	Select the preferred coder in the drop-down list for a local network address.
• Enable T.38	Select this check box to enable T.38 Fax-over-IP protocol.
• Enable SRTP	Select this check box to enable encrypted media streams.
• Media Relay	Select this check box to allow RTP-DTMF interoperability between H.323 and SIP devices
• No DTMF Detection	Select this check box to send DTMF tones in-band through the media channel but not as separate signalling messages.
• Record to (URL)	HTTP url where the recording file is to be stored. HTTP server must allow write access (PUT) at this location. One PCAP file is written for every call via this interface containing both RTP streams. Audio streams can be played using Wireshark.

SIP Interop Tweaks

• Proposed Registration Interval [s]	Set in seconds, default is 120 seconds. A value too low increases the network load.
• Accept INVITE's from Anywhere	Check this box to accept invites from anywhere, not only from the proxy configured.
• Enforce Sending Complete	Affects handling of "484 Address Incomplete" responses. If enabled and "484 Address Incomplete" is received, the call is cleared. If not enabled and "484 Address Incomplete" is received, the call is retained and re-initiated in case of new dialing digits.
• From Header when Sending INVITE	Interoperability option for outgoing calls. This controls the way CGPN is transmitted to the SIP provider. Possible values are: - Fixed AOR - The From header contains the fixed registration URI (AOR). The actual calling party number and name will be transmitted inside the P-Preferred-Identity header (RFC 3325). - AOR with CGPN as display - The From header contains the fixed registration URI (AOR) with the calling party number as display string in front of the AOR. - CGPN is user part of URI - The From header contains an URI with the calling party number as user part (left from @).

• Identity Header when Sending INVITE	Interoperability option for outgoing calls. This controls the way CGPN is transmitted to the SIP provider. Possible values are: - CGPN is user part of URI - The Identity header contains an URI with the calling party number as user part (left from @). - Fixed AOR - The Identity header contains the fixed registration URI (AOR). The actual calling party number and name will be transmitted inside the P-Preferred-Identity header (RFC 3325).
• Reliability of Provisional Responses	This controls the way the option tag "100 rel" is offered. Possible values are: - Supported - The tag is an optional extension. - Required - The tag is a mandatory extension. - Disabled - The tag is not offered.
Internal Registration	
• Protocol	Select "None" in the drop-down list, which is the default value.

4 Click "OK".

Call Number (CGPN/CDPN) Mappings

For every interface, it is possible to store mappings for CGPN In, CDPN In, CGPN Out and CDPN Out (explained in the table below), enabling call numbers and call number formats to be adjusted for incoming and outgoing calls.

Call Number Mappings Table

Map name	Description	Used to
CGPN In	Calling Party Number In	edit the calling number of incoming calls
CDPN In	Called Party Number In	edit the called number of incoming calls
CGPN Out	Calling Party Number Out	edit the calling number of outgoing calls
CDPN Out	Called Party Number Out	edit the called number of outgoing calls

1 Select Gateway > SIP.

2 For the interface that you want to set up call number modifications on, click the "+" sign next to the interface name. A new window opens and call number mapping can be made for the interface.

3 Select one of the following mapping lines.

Field name	Description
• CGPN in	if you want to edit the calling number of incoming calls. Digits used for the headmatch on the received number. In addition to the normal dialling digits (0..9,*,#) the following characters have special meaning: R If 'R' is used as first digit of the number only numbers with 'presentation restricted' match. In this case the 'presentation restricted' property is cleared if 'R' is not used on 'Number Out'. ? Can be used at any place inside the number and means that any received digit matches.

- CGPN out If you want to edit the calling number of outgoing calls.
- CDPN in If you want to edit the called number of incoming calls.
- CDPN out If you want to edit the called number of outgoing calls.

4 On each mapping line, a Call Number Type can be selected from the Call Number Type drop-down list (found on the righthand side of the lines).

NOTE: This step is optional.

Possible values are:

- Unknown: The mapping applies to unknown, external calls
- ISDN: The mapping applies to external calls
- Private: The mapping applies to internal calls

5 On each mapping line, a Call Number Format can be selected from the Call Number Format drop-down list (found on the lefthand side of the lines).

NOTE: This step is optional.

The table below describes of the possible values:

Call Number Formats Table

Name	Description	Typical use	Abbreviation
Unknown	Unspecified	Called number in outgoing calls	u
Subscriber	Call number in local network	Number called in incoming calls.	s
National	Call number with area code.	Calling number from home country.	n
International	Call number with country code and area code.	Calling number from abroad.	i
Abbreviated:	Unusual.		a
Network-specific	Unusual.		x

6 Click “OK”.

8.13.4 Gatekeeper Interfaces

Gatekeeper (GK) interfaces are channels to the world of Voice over Internet Protocol (VoIP). If your IP-DECT system needs to communicate with other devices via VoIP, access to these devices can be configured as a Gatekeeper interface.

Note: Normally the Master connects to a PBX via H.323/SIP endpoint registrations. In that case, no configuration in this section is needed.

These can be different types of equipment:

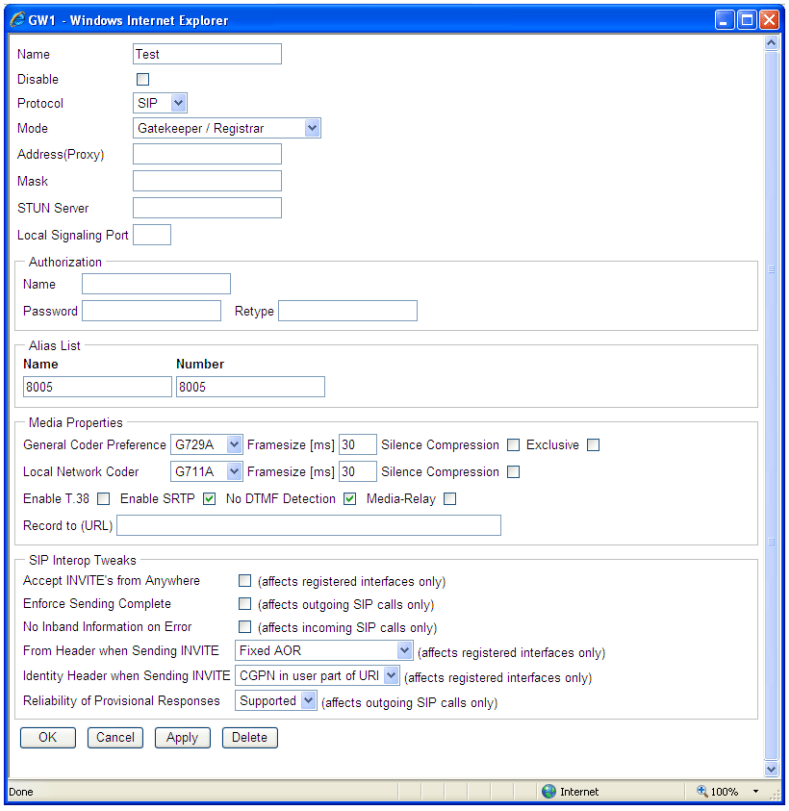
- Remote PBX
- Ascom VoIP Gateways
- VoIP terminal equipment
- VoIP terminal adapters to connect analogue terminals or a IPBS

- Third-party VoIP Gateway, as a gateway to telephone switches or, for example, into the SS7 network
- Further gatekeepers for call control
- VoIP PC programs

Each Gatekeeper interface defines access to a group of devices, which are all treated similarly. This allows, for example, all VoIP devices at one location to be configured via a single Gatekeeper interface. Since IP-DECT allows the definition of 12 different groups, it is able to communicate in all with several hundred VoIP devices.

1 Click Gateway > GK.

2 Click the desired interface name to be configured. A new window opens.



3 Select/Enter following settings.

Field name	Description
• Name	Enter a name for the route.
• Disable	Select the Disable check box to disable the route
• Protocol	Select one of the values below in the Protocol drop-down list. Possible values are: - H.323 - Selecting "H.323" (default) results in the GUI displaying a H.323 registration section and a *H.323 Interop Tweaks section*, both described below. - SIP - Selecting "SIP" results in the GUI displaying a SIP registration section and a *SIP Interop Tweaks section*. See8.13.3 *SIP Interfaces* on page 115 for a description of these sections.

• Mode	Select one of the values below in the Mode drop-down list. Possible values are: - Gateway without Registration - connects to the VoIP interface (gateway) to the configured gatekeeper without a registration. - Register as Endpoint - registers as VoIP terminal with the configured gatekeeper. - Register as Gateway - registers as VoIP gateway with the configured gatekeeper. - Gatekeeper / Registrar - accepts registrations from other VoIP devices. - ENUM - registers an ENUM connection with the relevant interface.
• Gatekeeper address (primary)	IP adress of the remote VoIP device
• Gatekeeper address (secondary)	It is important to enter an alternative gatekeeper IP address, especially when using redundant systems.
• Mask	Enter network mask
• Gatekeeper Identifier	In general, you can operate without Gatekeeper ID if only one gatekeeper is operated in your network or if Gatekeeper discovery is not used.
Authorization	Use these settings if log on to another gatekeeper is needed.
• Password	The Password corresponds to the H.235/SIP password required for logging on to the remote gatekeeper.
• Retype	Confirm password
Alias list	
• Name	Define the H.323/SIP name required to identify yourself with the gatekeeper. This is the "Long name" on the PBX *Show* area.
• Number	Usually the gateway only registers with a H.323/SIP name and not with an E.164 address (i.e. with a telephone number). Refer to the documentation for the gatekeeper you want to register.
Media properties	For information on these settings see *Media Properties* on page 116.
H.323 Interop Tweaks	
• No Faststart	Enable if the H245 Faststart procedure is to be disabled.
• No H.245 Tunneling	A TCP connection of its own is established for the voice data connection negotiation. Only recommended if compatibility problems occur with third party products.
• Supress HLC	Suppresses the transmission of "high layer compatibility" information elements on the interface.
• Supress FTY	Suppresses the transmission of "facility information elements" on the interface.

- Supress Subaddress — Suppresses the transmission of "Subaddresses" on the interface.

4 Click "OK".

Call Number Mappings

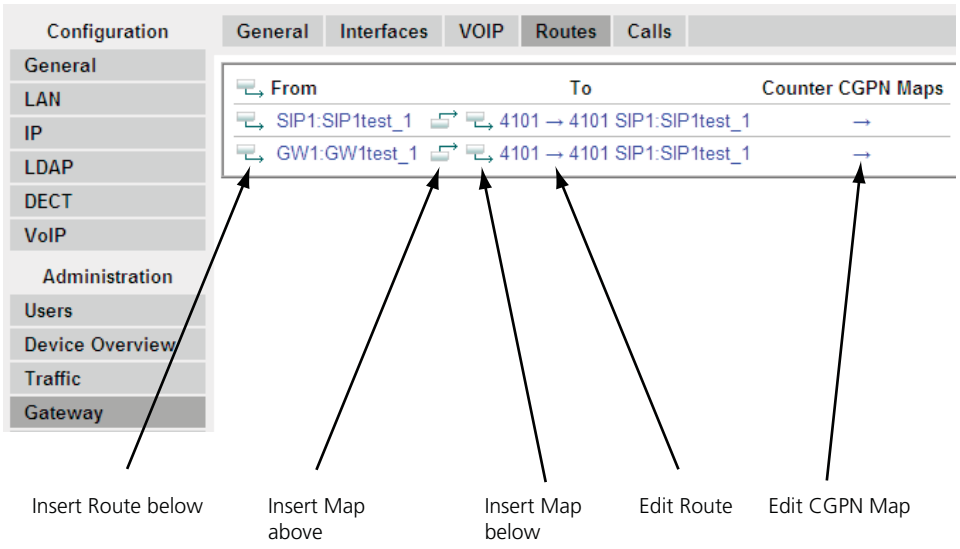
Call number (CGPN/CDPN) mappings are described in *Call Number (CGPN/CDPN) Mappings* on page 118.

8.13.5 Routes – Configuration

Call routing determines which calls are able to be accepted by the gateway and where they are to be switched.

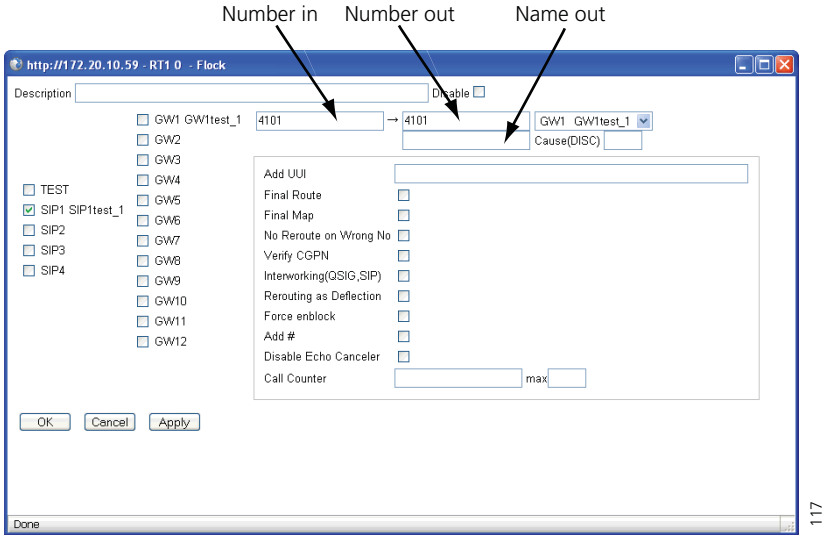
1 Select Gateway > Routes.

All configured routes are shown in a routing table.



2 **a.** If no routes have been configured, click on the in front of From.

b. Add a new route by clicking on the leftmost in the route which you want to insert the new route after.
Note the order of the routes here. The new route is always inserted after the current entry. A new window opens.



3 Select the check boxes of the VoIP interfaces in the left area, to mark them as valid sources for this route. Select interfaces which have been configured.

4 In the drop-down list in the right area, select the destination to which the calls are to be connected. Select interfaces which have been configured.

5 Select/Enter the following settings:

Field name	Description
• Description	Enter a name for the route. This will help you maintain an overview later on.
• Number in	Enter the dial prefix the route shall be valid for. Number in can be used in two ways: Pre and Post dial. We can use the following special characters here: - the period . - the question mark ? - and the exclamation mark ! 42.3 ignores the 3 and will use any number in starting with 42, of length 4 42?3 will allow the following numbers [4203,4213,4223,4233,4243,4253,4263,4273,4283,4293]
• Number out	Enter the replacement for the dial prefix that you specified in the “Number in” field. Simply copy the dial prefix into this field if the call number is to be adopted unchanged. Add an “!” to the number if a route is to apply to a certain number and all of the digits subsequently dialled are to be ignored.
• Name out	
• Add UUI	If manufacturer-specific data is to be transmitted in the signalling channel, for example, the URL for an announcement, this URL (e.g. “http://www. ...“) can be entered here.

Leave all the remaining fields blank, in the normal case.

- Final Route — Enable if the routing shall stop here
- Final Map — Enable if the mapping shall stop here.
- No Reroute on wrong No — Enable if you don't want to reroute when call fails due to wrong number.
- Verify CGPN — Map will match only if there is a matching CGPN map too.
- Interworking (QSIG, SIP) — Enable to support supplementary services (such as name display, call transfer, call diversion etc.)u between the H.323/SIP network and a QSIG network.
- Rerouting as Deflection — Enable if "call rerouting" supplementary service shall be implemented as "call deflection".
- Routing on Diverting No — Enable if routing shall be done based on diverting number (diverting leg2 info).
- Force enblock — Enable to send call en-block after 4 seconds interdigit timeout.
- Add # — A # can be transmitted to mark the end of the call number. This is required for devices, such as from Cisco, which are unable to identify the end of a number properly.
- Disable Echo Canceler
- Call Counter — A name for resource management can be entered.
- Max — Limits the number of permitted calls for a route.

6 Click "OK"

If, by way of exception, the route for a Map entry is to be configured with a different destination than that specified in the route's destination field, you can select this from the Destination field of the "Map".

Add CGPN map

1 Select Gateway > Routes.

2 For the interface, that you want to add a CGPN map, click the "->" sign under the CGPN map heading.

A new window opens.

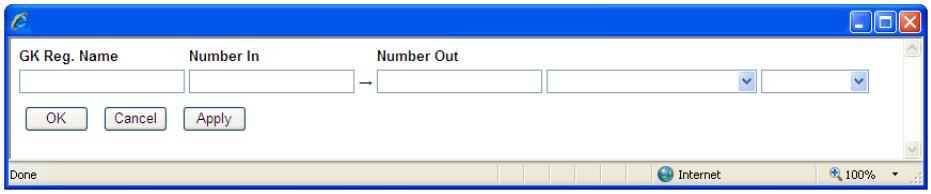


Figure 31. Number In – Number Out

3 Under "Number in" define the number type and –prefix that you wish to have replaced. The number type is denoted using the abbreviation from the Call Number Formats Table (see *Call Number Formats Table* on page 119).

4 Define the substitution under "Number out".

5 Click "OK".

Note: All call numbers in IP-DECT are always processed in "unknown" format. That is why the result of a number replacement for incoming calls, always is of the type "unknown" and the call number type of outgoing calls to be replaced is likewise always "unknown". Accordingly, you cannot specify a number type for replacements of incoming numbers in the "Number out" field and for replacements of outgoing numbers in the "Number in" field.

8.13.6 Show Active Calls

Select Gateway > Calls.

On this page you can see the currently active calls on all configured gateway interfaces. Calls from the IP-DECT Master does not normally display here.

The individual columns are explained in the table below.

Column	Format	Values	Description

Interfaces	sif:cgpn:cgnm ->dif:cdpn:cdnm/ ccn		Sif: Interface for incoming call. Cgpn: calling number, before routing. Cgnm: calling name before routing. Dif: Interface for the outgoing call. Cdpn: called number after routing. Cdnm: called name after routing. ccn: Name of the call counter used for this route (call counter name).
Protocols	AProtocol/BProtocol		The protocol used on the calling and the called side.
Coders	ACoders/BCoders Coder,ms (round, jitter)		Encoder used from A to>B or B to> Coder: voice compression used. ms: packeting used. round: Transmission duration in ms. jitter: Variance of transmission delay in ms.
Numbers	Caller->Called	Caller Called	The number of the caller as transmitted to the call destination. The number dialled.
Uptime	d:h:m:s		The uptime of the call in days, hours, minutes and seconds.
State		Dialling Alerting Connected Clearing	Dialling is in progress. The dialled distant terminal is being called. The call is connected. The call has been terminated by one of the two parties.

8.14 Backup

The IPBS/IPBL configuration can be downloaded and saved on a disc or a server. This is useful when identical configuration should be applied to several IPBSs/IPBLs, for example when configuring the Radios in a system. For information on how to load a saved configuration on the IPBS/IPBL, see 8.18 *Update* on page 130.

1 Select Backup > Config.

2 Click "download".

Click "download with standard password" to save the configuration with the default system password.

3 Click "Save" in the dialogue window and browse to the place where the configuration should be saved.

4 Click "Save".

8.15 Software Upgrade

Note: In software version 5.0.x:
The RFP version information is not displayed in the IPBS2 GUI. RFP software is more integrated now and this information becomes obsolete. In IPBS1 the RFP software has a separate flash memory, but this is not the case for IPBS2. On the IPBS1 the RFP version is still displayed.

8.15.1 Before Upgrading

1 For safety, take a backup of the configuration parameters for the Master and Standby Master.

2 Make a note of the Master and Standby Master IP address.

On the device configured as Master, continue with step 3 to 6 below.

3 When upgrading from software version 2.x.x to later: Select DECT > SMS and make a note of the IMS3 IP address.

4 When upgrading from software version 2.x.x to later: Select DECT > Master and make a note of the SIP proxy (registrar) IP address, found in the Gatekeeper IP Address text field.

5 When upgrading from software version 2.x.x to later: Select DECT > Master and make a note of the alternative SIP proxy (registrar) IP address, found in the Alt. Gatekeeper IP Address text field.

8.15.2 Upgrading Sequence

The best order is to start with the firmware and boot file upgrade of the Standby Master, then the Master, then all Radios, then do the configuration changes. This way the Radios will not be able to connect to the Master or Standby Master with incompatible firmware. The upgrading sequence is as follows:

1 Upgrade firmware and boot file of Standby Master, see *8.15.3 IPBS/IPBL Upgrade*.

2 Upgrade firmware and boot file of Master, see *8.15.3 IPBS/IPBL Upgrade*.

3 Upgrade firmware and boot file of Radios, see *8.15.3 IPBS/IPBL Upgrade*.

4 When upgrading from software version 2.x.x to later: Update configuration of Radios, see *8.15.4 Configuration After Updating the Firmware From Software Version 2.x.x to Later*.

5 When upgrading from software version 2.x.x to later: Update configuration of Master, see *8.15.4 Configuration After Updating the Firmware From Software Version 2.x.x to Later*.

6 When upgrading from software version 2.x.x to later: Update configuration of Standby Master, see *8.15.4 Configuration After Updating the Firmware From Software Version 2.x.x to Later*.

7 When upgrading from software version 3.x.x to later: Update configuration of Master and Standby Master, see *8.15.5 Configuration After Updating the Firmware From Software Version 3.x.x to Later*.

8.15.3 IPBS/IPBL Upgrade

This section describes how to upgrade the IPBS/IPBL software versions 2.x.x, 3.x.x and 4.x.x as follows:

- From software version 2.x.x to 3.x.x, from 2.x.x to 4.x.x and from 2.x.x to 5.0.x.
- From software version 3.x.x to 4.x.x and from 3.x.x to 5.0.x.
- From software version 4.x.x to 5.0.x.

1 When upgrading from software version 2.x.x to later: Disable LDAP replication for all Radios except in the case of Standby Master to Master Replication. Select LDAP > Replicator and make sure that the Enable check box is not selected.

2 Only for IPBL: When upgrading from software version 2.x.x to later: Update the boot file to 413. See *8.18.3 Update the Boot File* for more information on how to update the boot file.

3 When upgrading from software version 2.x.x to later: Update the firmware to 2.4.0 or later 2.x.x. See *8.18.2 Update Firmware* for more information on how to update the firmware.

4 Reset in order to make the changes take effect, see *8.22 Reset*.

5 Update the firmware to 3.x.x, 4.x.x or 5.0.x. See *8.18.2 Update Firmware* for more information on how to update the firmware.

6 When upgrading from software version 2.x.x to later: Reset in order to make the changes take effect, see *8.22 Reset*.

7 Update the boot file to 5.0.x. The boot file version contains a built-in web server, so there is no need to use the Gwload tool (a tftp-style client used to repair a broken firmware) if the IPBS is unreachable through the web GUI. See *8.18.3 Update the Boot File* for more information on how to update the boot file.

8 Reset in order to make the changes take effect, see *8.22 Reset*.

9 To update the IPBS Web GUI, press CTRL+F5 on the keyboard or close the IPBS Web GUI and start it again in order to update the GUI.

8.15.4 Configuration After Updating the Firmware From Software Version 2.x.x to Later

The following configuration settings should be changed in the Web GUI after updating the firmware from version 2.x.x to later.

Radio Configuration

1 Select DECT > Radio and enter the name and password for the Pari Master.

2 Reset in order to make the changes take effect, see *8.22 Reset*.

Master/Standby Master Configuration

For both Master and Standby Master, do as follows:

1 If the Radio is activated, select DECT > Radio and enter the name and password for the Pari Master in the Name and Password text fields.

2 For Standby Master only: Enter the address to the Master in the Primary Master IP Address text field.

3 Select UNITE > SMS and enter the address to the IMS3 in the IP Address text field.

4 Select DECT > Master.

5 Select the Enable Pari function check box.

If SIP protocol is used, continue with step 5 to 10 below:

6 Enter the IP address to the SIP proxy (registrar) in the Proxy text field.

7 Enter the IP address to the alternative SIP proxy (registrar) in the Alt. Proxy text field.

8 Select the Enbloc Dialing check box.

9 Select the Allow DTMF through RTP check box.

10 Select the Register with number check box.

11 To update the Web GUI, press CTRL+F5 on the keyboard or close the Web GUI and start it again in order to make the new menu to appear.

12 If H.323 protocol is used: Enter the address to the gatekeeper in the Gatekeeper IP Address text field.

13 Reset in order to make the changes take effect, see *8.22 Reset*.

8.15.5 Configuration After Updating the Firmware From Software Version 3.x.x to Later

Master/Standby Master Configuration

When upgrading from version 3.x.x to later the MWI will automatically be set to Off. If the MWI was enabled prior to the upgrade: Select DECT > Suppl. Serv. and select an MWI mode in the MWI Mode drop-down list.

When upgrading a system from software version 3.x.x to later, existing system administration accounts remain configured locally in the IPBS(s)/IPBL(s). However, it is recommended that the system administration accounts are configured centrally instead by moving them to the Kerberos server. To have the system administration accounts configured locally is a potential security risk. For information on how to configure Kerberos, see 8.1.3 *Centralized Management of Administrator/Auditor Accounts Using Kerberos* on page 61.

To move the system administration accounts to the Kerberos server, do as follows:

Step 1: For each IPBS/IPBL where system administration accounts have been configured locally, do as follows:

1 Select General > Admin.

2 Go to the Additional Administrator and Auditor Accounts section.

3 Write down each accounts configuration data such as the user name, password (when known) and role.

Step 2: On the Kerberos server, do as follows:

1 Select General > Kerberos Server.

2 Go to the Users section and enter the configuration data for each account that was written down in step 1 above.

3 Click "OK".

Step 3: For each IPBS/IPBL where system administration accounts have been configured locally, do as follows to delete the local system administration accounts:

1 Select General > Admin.

2 Go to the Additional Administrator and Auditor Accounts section.

3 For each account row, select the Delete check box.

4 Click "OK".

All local system administration accounts are deleted and the Additional Administrator and the Auditor Accounts section is no longer visible. The system administration accounts are now instead configured centrally on the Kerberos server.

8.15.6 System Upgrade from Software Version 4.x.x to 5.0.x

Radios with software version 4.x.x will not be able to connect to a Pari Master with software version 5.0.x. It is therefore recommended when doing a manual upgrade (i.e. when not using an update server) to upgrade Radios first and then the Pari Master.

8.16 System Downgrade from software version 5.0.x to 2.x.x, from 4.x.x to 2.x.x and from 3.x.x to 2.x.x

If a system with 3.x.x, 4.x.x or 5.0.x firmware and boot file is downgraded to a 2.x.x version, the HTTP server part of the boot code is removed.

If the firmware is downgraded to version 2.x.x, the LDAP replication must be activated again.

1 Select LDAP > Replicator.

2 Select the Enable check box to activate LDAP replication.

3 Check the MWI settings.

8.17 System Downgrade from software version 5.0.x to 3.x.x and 4.x.x to 3.x.x

After downgrading: Check the MWI settings.

8.18 Update

This section describes how to do the following configurations and settings.

- Update Configuration
- Update Firmware
- Update the Boot File
- Update the RFPs

8.18.1 Update Configuration

A previously saved configuration can be loaded and activated on the IPBS/IPBL. See 8.14 *Backup* on page 126 for information on how to save a configuration.

1 Select Update > Config.

2 Click "Browse..." and browse to the saved configuration.

3 Click "Upload".

4 Reset in order to make the changes take effect, see 8.22 *Reset* on page 138.

Note: If the IPBS2 is configured and the configuration is taken from IPBS1, some lines in the configuration will be skipped by IPBS2. This is because it is different hardware in IPBS1 and IPBS2 and some configuration lines are not applicable in IPBS2.

8.18.2 Update Firmware

The software can be updated. Follow the steps below to update IPBS/IPBL with the firmware. Download firmware from the IP-DECT system provider.

Note: If this operation is interrupted, the firmware in the device will be defect. If a firmware upload is for any reason interrupted, the firmware must be uploaded again. Do not execute a reset before the firmware upload is complete. For information on how to load new firmware if the IPBS/IPBL is unreachable through the web GUI, see 10.1 *Load Firmware Using the Gwload Tool* on page 142.

1 Select Update > Firmware.
2 Click "Browse..." and browse to the firmware file.
3 Click "Upload"
4 Reset in order to make the changes take effect, see 8.22 *Reset* on page 138.

8.18.3 Update the Boot File

1 Select Update > Boot.
2 Click "Browse..." and browse to the boot file.
3 Click "Upload".
4 Reset in order to make the changes take effect, see 8.22 *Reset* on page 138.

8.18.4 Update the RFPs

This section only applies to the IPBL.

The firmware can be updated. Follow the steps below to update RFP. Download firmware from the IP-DECT system provider.

In the RFP status list, information on connected RFPs are displayed.

1 Select Update > RFPs.
2 Click "Browse..." and browse to the RFP update file.
3 Click "Upload".

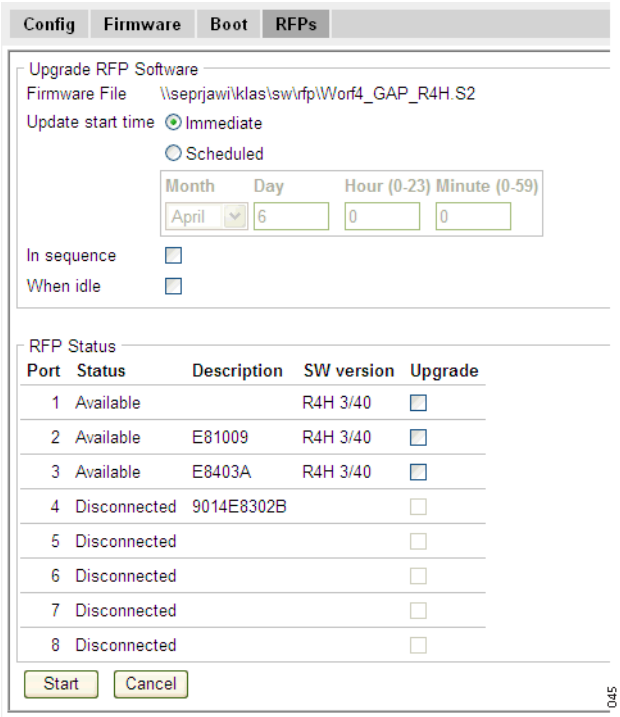


Figure 32. Upgrade the RFP

4 Select "Immediate" or "Scheduled" update.

5 Select "In sequence" check box to update the selected RFPs one by one.

6 Select "When idle" check box to start the update when the RFP is idle.

7 Mark the applicable RFPs to be updated.

8 Click "Start" to upgrade the selected RFPs.

The RFP restarts after the upload is finished.

8.19 System Upgrade in System with Mobility Masters

Upgrade in the following order:

1 Upgrade all Standby Mobility Masters.

2 Upgrade all Mobility Masters.

3 Upgrade all of the remaining devices for each site by following the upgrade sequence under 8.15.2 *Upgrading Sequence* on page 127.

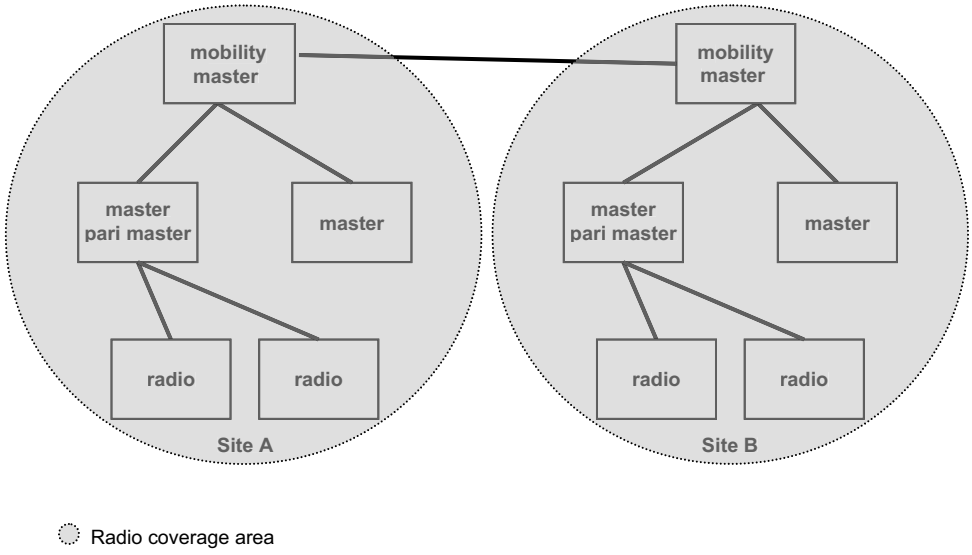


Figure 33. System with several Mobility Masters

Following limitations apply during upgrade:

- *Using software version 3.x.x at site A and software version 4.x.x at site B:*
  - 3.x.x users get No Access when located in site B (4.x.x).
  - Idle display does not work for 4.x.x users located in site A (3.x.x software).

- *Using software version 3.x.x at site A and software version 5.0.x at site B:*
  - 3.x.x users get No Access when located in site B (5.0.x).
  - 5.0.x users get No Access when located in site A (3.x.x).

- *Using software version 4.x.x at site A and software version 5.0.x at site B:*
  - 5.0.x users get No Access when located in site A (4.x.x).

8.20 Replacing Master Hardware in Multiple Master System

If a faulty Master IPBS is replaced with a new one and the same configuration shall be applied to the new one, then the faulty Master must have been disconnected from the system more than 2 minutes before the new Master is connected, otherwise all the subscription data will be lost.

For information on how to load a configuration on the new Master, see 8.18.1 *Update Configuration* on page 130.

8.21 Diagnostics

8.21.1 Logging

The IPBS/IPBL can generate a number of logs which can be useful when supervising and troubleshooting the IP-DECT system. For information on how to collect the log files, see 8.1.6 *Configure Logging* on page 69. For a description of each log, see the table below.

Setting	Description
TCP	Logs generated upon TCP connection set-ups in the H.225 / H.245 protocol.
Gateway Calls	Logs generated by calls that go through the gateway interface.
Gateway Routing	Logs generated by calls that are routed through the gateway interface.
H.323 Registrations	Logs generated upon RAS registration.
SIP/UDP Registrations	Logs generated upon SIP registration.
SIP/TCP Registrations	Logs generated upon SIP registration.
SIP/TLS Registrations	Logs generated upon SIP registration.
DECT Master	Logs generated by the Master software component in the IPBS/IPBL.
DECT Radio	Logs generated by the Radio software component in the IPBS/IPBL.
DECT Stack	A low level DECT log, intended for support departments.
Config Changes	Logs generated upon configuration changes in the IPBS/IPBL or the IP-DECT system.
Radio is busy for speech	Enable if a fault event should be sent when all speech resources are busy.

1 Select Diagnostics > Logging.

2 Select which logs to generate by selecting the check box next to the log name.

3 Click "OK".

4 View the logs by clicking the "syslog" link. The logs are updated in real-time.

8.21.2 Tracing

The information gathered from the trace functionality is mainly used for troubleshooting in case of failure in the system. The trace information is intended for the support departments.

It is possible to trace traffic information on the LAN for troubleshooting purposes.

1 Select Diagnostics > Tracing.

2 Select the *Enable* check box in the *Remote PCAP* section to enable the use of a network protocol analyzer program, for example Wireshark.

The *Trace* check box in the *Remote PCAP* section is mainly used by the R&D department to follow the desired network attributes.

3 Select the *TCP/UDP Traffic* check box in the *IP* section to capture traffic information.

4 Click "OK".

8.21.3 Alarms

Under Diagnostics > Alarms are all active alarms displayed.

An alarm is a fault that affects the normal service of the IP-DECT system and may require action from personnel to correct it. An IP-DECT Master can collect alarms from Radios and it can display all active alarms in the system. If an object is removed from the system,

object-related alarms are automatically cleared after a timeout period of 30 minutes. Active alarms are also cleared if the related object is restarted.

For a description of the attributes, see the table below.

Attribute	Description
Time	The date and time when the alarm is issued.
Code	A unique number that identifies the alarm. Click the code to get more detailed information about the alarm. For a list of possible codes and their descriptions, see 10.2 *Fault Code Descriptions* on page 142.
Severity	It has three possible states: • Critical - Immediate action is required. It is displayed, for example, if a managed object goes out of service. • Major - Urgent action is required. It is displayed, for example, if the capability of the managed object is severely degraded. • Indeterminate - Level of severity cannot be determined
Remote	The IP Address of the object that reported the alarm. Click the IP address to access the object.
Source	The software module that reported the alarm. Together with the code it uniquely identifies an alarm.
Description	A textual description of the alarm.

8.21.4 Events

Under Diagnostics > Events is history of alarms and errors displayed including active alarms. Click "Clear" in the top-right corner to clear the list of alarms and errors.

For a description of the attributes, see the table below.

Attribute	Description
Time	The date and time when the alarm, error is issued or cleared.
Type	The status of the fault. It has four possible states: • Alarm - Alarms displayed in red are active alarms • Alarm cleared - The alarm is already cleared • Alarm timeout - The alarm exceeded the timeout period • Error - Refers to faults that are not active for a specific time.

Code	A unique number that identifies the alarm. Click the code to get more detailed information about the alarm. For a list of possible codes and their descriptions, see 10.2 *Fault Code Descriptions* on page 142.
Severity	It has three possible states: • Critical - Immediate action is required. It is displayed, for example, if a managed object goes out of service. • Major - Urgent action is required. It is displayed, for example, if the capability of the managed object is severely degraded. • Indeterminate - Level of severity cannot be determined
Remote	The IP Address of the object that reported the alarm. Click the IP address to access the object.
Source	The software module that reported the alarm. Together with the code it uniquely identifies an alarm.
Description	A textual description of the alarm.

8.21.5 Performance

It is possible to check different performance parameters. For a description of the parameters, see the table below.

Parameter	**Description**
CPU	Shows CPU utilization
CPU-R	Shows utilization of CPU resources allocated by different tasks
MEM	Shows memory utilization
Concurrent calls	Shows the number of ongoing calls
Temperature (only for IPBL)	Shows the temperature of the cabinet
Voltage (only for IPBL)	Shows the power supply voltage level
Current (only for IPBL)	Shows the power supply current consumption

1 Select Diagnostics > Performance

2 Select the checkbox(es) for the desired performance statistics.

3 Click "OK".

4 One window shows statistics for the last 24 hours. The maximum possible value is displayed in the top-left corner. Click the left or right arrow buttons to see different time frames.

8.21.6 Config Show

Under Diagnostics > Config Show, the configuration is displayed as a text output.

8.21.7 Ping

The ping function is used to determine the response time from the IPBS/IPBL to a certain IP address. It can be used to analyse the connection between the IP-DECT system components.

1 Select Diagnostics > Ping.

2 Enter an IP address in the IP Address text field.

3 Press "Enter" on the keyboard.

8.21.8 Traceroute

The traceroute function displays how packets travel from the IPBS/IPBL to a certain IP address. The result is an ordered list of IP addresses with the measured round trip time.

1 Select Diagnostics > Traceroute.

2 Enter an IP address in the IP Address text field.

3 Press "Enter" on the keyboard.

8.21.9 Environment

This section only applies to the IPBL.

The environment tab gives information power supply and consumption. It also display temperature and fan status.

1 Select Diagnostics > Environment.

2 The following information is available in the *Power* section:

- Power supply - AC or DC power port.
- Voltage - input voltage.
- Current consumption - total consumption for the IPBL an the connected RFPs.
  – Max 4,0 A when supplied with AC power port
  – Max 5,2 A when supplied with DC power port

3 The following information is available in the *Environment* section:

- Temperature - °C
- Fan status - OK, not OK

8.21.10 RFP Scan

This section only applies to the IPBS.

To scan for occupied system IDs of other IP-DECT systems within the coverage area, perform an RFP scan following the steps below.

Note: Executing an RFP scan will terminate all calls on the IPBS.

1 Select Diagostics > RFP Scan

2 Click "Start Scanning"

8.21.11 Service Report

To download a service report do the following:

1 Select Diagnostics > Service Report.

2 Click "download".

3 Click “Save” and browse where to save the service report.

8.22 Reset

Some configuration changes requires a reset in order to take effect. A reset reboots the software. There are two ways to perform a reset:

- Idle reset - waits until there are no active calls in the IPBS/IPBL.
- Immediate reset - clears all calls and resets the IPBS/IPBL.

8.22.1 Idle Reset

1 Select Reset > Idle Reset.

2 Click "OK".

3 The IPBS/IPBL will reset when there are no active calls.

8.22.2 Immediate Reset

1 Select Reset > Reset.

2 Click "OK".

3 The IPBS/IPBL will terminate all active calls and reset.

8.22.3 TFTP Mode

Note: When the IPBS/IPBL is in TFTP mode it can only be reached using the *gwload* utility. This mode should not be used during normal operation.

8.22.4 Boot

When the IPBS/IPBL is in Boot mode it uses a small version of the firmware (minifirmware) which contains only the IP stack and the web interface.

1 Select Reset > Boot.

2 Click "OK".

8.23 Reset Using the Reset Button

It is possible to do a hardware reset of the IPBS and IPBL by pressing the reset button. The button is accessed through a hole in the back of the IPBS (IPBS1: figure 1 on page 3, IPBS2: figure 2 on page 6) and on the front of the IPBL (figure 4 on page 10).

Note: Use a pointed object in an non conducting material to perform a reset.

Short press < 1 sec	Restart
Medium press ~3 sec. For IPBS2: When 3 sec. has gone, the LED on IPBS2 will start to flash in blue and the reset button can then be released.	Restart in TFTP mode. In TFTP mode the IPBS and IPBL can be accessed only through the gwload application. This mode is intended for support and development departments.

Long press ~ 10 sec. For IPBS2: When 10 sec. has gone, the LED on IPBS2 will start to flash in blue, indicating the start of the factory reset process. Hence the reset button can then be released. When the LED (LED 1 for IPBS1) is steady amber/ yellow, the factory reset process is complete. The device can now be restarted by disconnecting the supply voltage.	Factory reset - all configuration parameters will be set to default values.

9 Commissioning

This section describes the visual inspection and tests that must be executed after completing the installation and initialization of the IP-DECT system. The purpose of the visual inspection and tests is to verify that all installation activities have resulted in a correctly functioning system. If it appears that a part is malfunctioning while the system is installed correctly (that is, no cabling faults, no configuration faults), the technician must consult the maintenance section included in this manual for fault finding.

9.1 Radio coverage verification tests

The radio coverage verification consists of two tests:

- Base station operation test
- Coverage area test

Note: Be sure that all batteries in the handset are charged before executing the tests.

9.1.1 Base Station Operation Test

The purpose of this test is to check if all base stations are operational.

1 Put a handset in the service display mode (DCA mode), see applicable User Manual for the handset.

2 Use the base station plan, see the applicable System Planning documentation for IP-DECT.

3 Move close to each base station and check that the handset locks to it (the service display should display the correct number).

After having checked that all base stations are operational proceed with the coverage area test.

9.1.2 Coverage Area Test

The purpose of this test is to verify that there is satisfactory field strength to enable good speech quality everywhere within the covered area (rooms, lift shafts, staircases). This test is executed with two handsets and requires two persons.

1 Place the handset in the service display mode (DCA mode) and call the other handset. One user of the handset should now start moving around the covered area. Both users must check that a good speech quality is maintained everywhere. Special attention should be paid to areas such as edges of the building and areas behind metal structures where there is a possibility of reduced speech quality.

2 Mark areas where cracking sounds or mutes are heard.

9.1.3 Evaluation

After having performed the coverage area test, the results should be evaluated. If the coverage is not sufficient you should review the planning and move or add equipment.

9.2 Cordless Extension Number Test

This test checks for each handset the complete connection from the IP-DECT system to the PBX. Furthermore it checks that the handsets' numbers have been correctly programmed. The test is performed by calling all handset from one specific handset.

1 Put all handset together in order of extension number on a table.

2 Go off-hook with each handset and check that the dial tone is heard.

3 Call with a handset (handset A) all other handsets sequentially and check that the handset with the corresponding number on its display rings when called.

4 Call handset A and check if it rings.

10 Troubleshooting

10.1 Load Firmware Using the Gwload Tool

If the firmware is corrupt, for example if firmware download is interrupted the IPBS/IPBL could become unreachable by the web GUI. It will not be possible to load new firmware or to start correctly. If this occurs, the IPBS/IPBL runs on the bootcode and the Gwload tool (a tftp-style client used to repair a broken firmware) can be used to upload firmware.

1 Download the Gwload software from the IP-DECT system provider.

2 Set the IPBS/IPBL in TFTP-mode by performing a medium (~3 sec) hardware reset, see *8.23 Reset Using the Reset Button* on page 138.

3 Start a command window.

To update with wew firmware, execute the following command from the folder where the gwload.exe file is located:

IPBS:
gwload /setip /i <ipaddress> /gwtype 1201 /prot <..path/firmwarefilename> /go

IPBL:
gwload /setip /i <ipaddress> /gwtype 4001 /prot <..path/firmwarefilename> /go

4 If there is more than one IPBS/IPBL in TFTP mode, select the unit to update and press enter.

10.2 Fault Code Descriptions

This section lists the possible fault codes, their description and severity level.

Explanation of the table columns **C**, **M** and **I**:

C = Critical (IP-DECT) / Critical (Unite)
M = Major (IP-DECT) / Error (Unite)
I = Indeterminate (IP-DECT) / Warning (Unite)

Description	Code	Device	C	M	I
Interface down (Gateway)	0x00010001	IPBS/IPBL		X	
Registration down (Gateway)	0x00010002	IPBS/IPBL		X	
Protocol error (Gateway)	0x00010003	IPBS/IPBL		X	
The LDAP replicator is not connected (Users)	0x00030001	IPBS/IPBL		X	
CPU resources are not available (Radio)	0x00030101	IPBS/IPBL			X
Standby master active (Master)	0x00030201	IPBS/IPBL		X	
User registration failure (Master)	0x00030202	IPBS/IPBL		X	
Emergency registration down (Master)	0x00030203	IPBS/IPBL		X	
Connection to Radio lost (Master)	0x00030204	IPBS/IPBL		X	
Primary/redundant trunk is down (Master)	0x00030205	IPBS/IPBL		X	
Connection to Mobility Master lost (Mobility Master)	0x00030301	IPBS/IPBL		X	
Cannot establish connection to Mobility Master (Mobility Master)	0x00030302	IPBS/IPBL		X	
Connection to Master lost (Mobility Master)	0x00030303	IPBS/IPBL		X	

Standby Mobility Master is active (Mobility Master)	0x00030304	IPBS/IPBL		X	
No Media data received (RTP)	0x00050001	IPBS/IPBL		X	
Excessive loss of data (RTP)	0x00050002	IPBS/IPBL		X	
Wrong payload type received (RTP)	0x00050003	IPBS/IPBL		X	
Stun failed (RTP)	0x00050004	IPBS/IPBL		X	
SRTP authentication failed (RTP)	0x00050005	IPBS/IPBL		X	
SRTCP authentication failed (RTP)	0x00050006	IPBS/IPBL		X	
Unexpected message (H323)	0x00060001	IPBS/IPBL		X	
Status inquiry (H323)	0x00060002	IPBS/IPBL		X	
Signaling TCP failed (H323)	0x00060003	IPBS/IPBL		X	
Signaling timeout (H323)	0x00060004	IPBS/IPBL		X	
NAT discovery failed (SIP)	0x00070001	IPBS/IPBL		X	
Overload (SIP)	0x00070003	IPBS/IPBL		X	
Coder selection failed (SIP)	0x00070004	IPBS/IPBL		X	
Media configuration failed (SIP)	0x00070005	IPBS/IPBL		X	
DNS failed (SIP)	0x00070006	IPBS/IPBL		X	
Invalid URL (WebMedia)	0x00080001	IPBS/IPBL		X	
Coder missing in URL (WebMedia)	0x00080002	IPBS/IPBL		X	
Unexpected restart (watchdog/reset/power on) (Cmd)	0x000b0001	IPBS/IPBL		X	
Unexpected message (TLS)	0x000c010a	IPBS/IPBL			X
Unexpected message (TLS)	0x000c020a	IPBS/IPBL			X
Bad MAC (TLS)	0x000c0114	IPBS/IPBL			X
Bad MAC (TLS)	0x000c0214	IPBS/IPBL			X
Decryption failed (TLS)	0x000c0115	IPBS/IPBL			X
Decryption failed (TLS)	0x000c0215	IPBS/IPBL			X
Record overflow (TLS)	0x000c0116	IPBS/IPBL			X
Record overflow (TLS)	0x000c0216	IPBS/IPBL			X
Decompression failure (TLS)	0x000c011e	IPBS/IPBL			X
Decompression failure (TLS)	0x000c021e	IPBS/IPBL			X
Handshake failure (TLS)	0x000c0128	IPBS/IPBL			X
Handshake failure (TLS)	0x000c0228	IPBS/IPBL			X
No certificate (TLS)	0x000c0129	IPBS/IPBL			X
No certificate (TLS)	0x000c0229	IPBS/IPBL			X
Bad certificate (TLS)	0x000c012a	IPBS/IPBL			X
Bad certificate (TLS)	0x000c022a	IPBS/IPBL			X
Unsupported certificate (TLS)	0x000c012b	IPBS/IPBL			X
Unsupported certificate (TLS)	0x000c022b	IPBS/IPBL			X
Revoced certificate (TLS)	0x000c012c	IPBS/IPBL			X
Revoced certificate (TLS)	0x000c022c	IPBS/IPBL			X
Expired certificate (TLS)	0x000c012d	IPBS/IPBL			X
Expired certificate (TLS)	0x000c022d	IPBS/IPBL			X

Unknown certificate (TLS)	0x000c012e	IPBS/IPBL			X
Unknown certificate (TLS)	0x000c022e	IPBS/IPBL			X
Illegal parameter (TLS)	0x000c012f	IPBS/IPBL			X
Illegal parameter (TLS)	0x000c022f	IPBS/IPBL			X
Unknown CA (TLS)	0x000c0130	IPBS/IPBL			X
Unknown CA (TLS)	0x000c0230	IPBS/IPBL			X
Access denied (TLS)	0x000c0131	IPBS/IPBL			X
Access denied (TLS)	0x000c0231	IPBS/IPBL			X
Decode error (TLS)	0x000c0132	IPBS/IPBL			X
Decode error (TLS)	0x000c0232	IPBS/IPBL			X
Decryption error (TLS)	0x000c0133	IPBS/IPBL			X
Decryption error (TLS)	0x000c0233	IPBS/IPBL			X
Export restriction (TLS)	0x000c013c	IPBS/IPBL			X
Export restriction (TLS)	0x000c023c	IPBS/IPBL			X
Protocol version (TLS)	0x000c0146	IPBS/IPBL			X
Protocol version (TLS)	0x000c0246	IPBS/IPBL			X
Insufficient security (TLS)	0x000c0147	IPBS/IPBL			X
Insufficient security (TLS)	0x000c0247	IPBS/IPBL			X
Internal error (TLS)	0x000c0150	IPBS/IPBL			X
Internal error (TLS)	0x000c0250	IPBS/IPBL			X
User cancelled (TLS)	0x000c015a	IPBS/IPBL			X
User cancelled (TLS)	0x000c025a	IPBS/IPBL			X
No renegotiation (TLS)	0x000c0164	IPBS/IPBL			X
No renegotiation (TLS)	0x000c0264	IPBS/IPBL			X
Service not found (Kerb client)	0x000c0403	IPBS/IPBL		X	
Kerberos server unreachable (Kerb client)	0x000c0406	IPBS/IPBL		X	
Kerberos cross realm failure (Kerb client)	0x000c0407	IPBS/IPBL		X	
Certificate validation is disabled until system time is set (X509)	0x000c1000	IPBS/IPBL			X
Certificate expired/Will expire soon (X509)	0x000c1001	IPBS/IPBL			X
RFP disconnected (TAM)	0x000e0001	IPBL		X	
RFP malfunctioning (TAM)	0x000e0002	IPBL		X	
RFP disabled (TAM)	0x000e0003	IPBL		X	
RFP software download (Dwl)	0x000e0004	IPBL		X	
RFP unsynchronized (RFPInit)	0x000e0005	IPBS		X	
Synchronization to reference system lost (RFPInit)	0x000e0006	IPBS		X	
Other DECT system with same sysid detected (RFPInit)	0x000e0008	IPBS		X	
Sync master failed to resynchronize to reference (RFPInit)	0x000e0009	IPBS		X	
High temperature (TAM)	0x000f0001	IPBL	X		
High power consumption (TAM)	0x000f0002	IPBL	X		
Supply voltage low (TAM)	0x000f0004	IPBL	X		
Supply Voltage High (TAM)	0x000f0008	IPBL	X		

Fan failure (TAM)	0x000f0010	IPBL		X	
Synchronization ring broken (Sync)	0x00100001	IPBL		X	
Reference synchronization signal lost (Sync)	0x00100002	IPBL		X	
Synchronization lost (Sync)	0x00100004	IPBL		X	
Unsynchronized to reference (Sync)	0x00100008	IPBL		X	
Interface down (ipproc)	0x00110000	IPBS/IPBL		X	
Interface not configured (ipproc)	0x00110001	IPBS/IPBL			X
DHCP server not responding (ipproc)	0x00110002	IPBS/IPBL		X	
Invalid UDP-RTP port base/range (ipproc)	0x00110019	IPBS/IPBL		X	
Invalid UDP-NAT port base/range (ipproc)	0x0011001a	IPBS/IPBL		X	
Invalid NAT port base/range (ipproc)	0x0011001b	IPBS/IPBL		X	
ARP poisoning detected (ipproc)	0x00110041	IPBS/IPBL		X	
Out of TCP/NAT ports (ipproc)	0x00110046	IPBS/IPBL		X	
Out of TCP ports (ipproc)	0x00110047	IPBS/IPBL		X	
TCP bind error (ipproc)	0x00110049	IPBS/IPBL		X	
Out of UDP/RTP ports (ipproc)	0x00110050	IPBS/IPBL		X	
Out of UDP ports (ipproc)	0x00110051	IPBS/IPBL		X	
UDP bind error (ipproc)	0x00110053	IPBS/IPBL		X	
No route to destination (ipproc)	0x0011005a	IPBS/IPBL		X	
No route to destination, if down (ipproc)	0x0011005b	IPBS/IPBL		X	
No route to destination, if unknown (ipproc)	0x0011005c	IPBS/IPBL		X	
No route to destination, if unconfigured (ipproc)	0x0011005d	IPBS/IPBL		X	
No route to destination, no gateway (ipproc)	0x0011005e	IPBS/IPBL		X	
No route to destination, loop (ipproc)	0x0011005f	IPBS/IPBL		X	
Memory Low (box)	0x00120001	IPBS/IPBL	X		
Radio busy for speech (Dect)	0x00140001	IPBS			X
Busy for speech (CLU)	0x00150001	IPBL			X
Failed to transfer Unite communication block (Unite)	0x001a0001	IPBS/IPBL			X

11 Related Documents

System Description, Ascom IP-DECT System	TD 92375EN
System Planning, Ascom IP-DECT System	TD 92422EN
Data Sheet, IP-DECT Base Station	TD 92370GB
Data Sheet, IP-DECT Base Station (IPBS2)	TD 92836EN
Data Sheet, IP-DECT Gateway	TD 92430GB
Configuration Manual FXO in Ascom IP-DECT System	TD 92529GB
Configuration Notes for Cisco Call Manager in Ascom IP-DECT System	TD 92424GB
Configuration Notes for Aastra MX-ONE in Ascom IP-DECT System	TD 92637GB
Configuration Notes for Ascom VoIP Gateway in Ascom IP-DECT System	TD 92642GB
Technical Product Manual, DCT1800-GAP	TD 92093GB

Document History

For details in the latest version, see change bars in the document.

Version	Date	Description
Ver. A	5 February 2009-02-02	First released version.
Ver. B	15 April 2009 2009-04-15	Updated 8.7 *UNITE* on page 103 and added information about device management and service discovery.
Ver. C	5 May 2010 2010-03-05	Updated 8.5.12 *Configure Supplementary Services* on page 92. Updated 8.5.27 *Configure Air Synchronization* on page 100. Updated 8.10.1 *Radios* on page 107. New 8.10.6 *Sync Lost Counter in IPBS* on page 110. New 8.11 *DECT Sync* on page 111. Updated 8.15 *Software Upgrade* on page 127.
Ver. D	3 September 2010	New 7.13.3 *Easy Registration* on page 58 Updated 8.1.3 *Centralized Management of Administrator/Auditor Accounts Using Kerberos* on page 61 Updated 8.5.2 *Set Subscription Method* on page 89 New 8.7.1 *Configure Messaging* on page 103 New 8.8 *Import and Export a Central Phonebook* on page 105 New 8.9.5 *Export the Users to a csv file* on page 107
Ver. E	26 January 2011	Several changes, see change bars.
Ver. F	28 October 2011	Several changes, see change bars.
Ver. G	15 December 2011	Several changes, see change bars.
Ver. H	15 February 2012	Several changes, see change bars.

Appendix A: How to Use the Update Server

A.1 Summary

Automatic update is based on configuration and firmware information stored on a standard web server and retrieved by the devices on a regular basis.

There are 2 modules in the device which work in tandem. The first is known as "UP0" and actually executes the upload and download of configuration information as well as the download of updated firmware. UP0 is controlled by commands as described below.

The second module is known as "UP1". It serves to poll a given website for changed configuration information. If certain conditions are met, UP1 will issue commands to UP0 to perform the requested updates.

UP0 can also receive commands from the "Update clients" page of the PBX Administration user interface.

A.1.1 System Requirements

One or more regular Web Server that can be accessed by all devices are required. This has been tested with Microsoft IIS and Apache, but any regular Web Server should do.

For best results, the Web Server should be able to maintain a large number of HTTP sessions simultaneously, since potentially all devices may attempt a configuration update at the same time. For example, Microsoft's Personal Web Server is not adequate, since it only support 10 simultaneous sessions.

Following URLs are supported: HTTP, HTTPS and TFTP.

A.1.2 Installation

To be able to upload (save) device configuration information on the web server, it must allow HTTP PUT requests. All other functions require HTTP GET permissions only.

Since all HTTP requests are performed unauthenticated, the website used must allow anonymous read (and potentially write) access. You may want to restrict access to that site to certain network address ranges.

Configure a Microsoft IIS URL to allow PUT commands:

1 Create a directory where you want to save configurations to

2 Create a virtual directory in Microsoft's IIS manager

3 Select "read" and "write" access

No installation is needed on the IPBS/IPBLs.

A.1.3 Configuration

See 8.1.4 *Configure Automatic Firmware Update* on page 68 on how to configure the IPBS/IPBLs for automatic update.

The URL parameter must point to the site where the file containing the maintenance commands is stored. Note that in this URL, no host names are supported. The web servers IP address must be used.

A.1.4 Setting the UP1 Parameters

The applet saves the configuration in a line starting config change UP1.

The full syntax is:

```
config change UP1 /url <url> [/poll <slow>] [/poll-fast <fast>]
[/disc]
```

If the URL ends with a '/' then a default filename is used based upon the product in question. If for example the URL is "http://1.2.3.4/configs/", it is expanded to "http://1.2.3.4/configs/update-IPBS.htm" (.../update-IPBL).

The product type name used is the one used in the Version line on the devices Info page. Note that the extension is irrelevant, .htm or .txt or no extension at all may be used. On some Web servers, URLs are case sensitive.

The maintenance command file is retrieved initially after the configured poll interval (in minutes) is expired after boot. Short poll intervals can create substantial load on a big network. A value less than 15 minutes (which is the default) is therefore not recommended.

However, for new devices (that is, devices which have been reset to factory settings and never had a successful download of a maintenance command file), the command file is retrieved every minute (for up to 30 minutes). This is done so that a fresh device can quickly retrieve a site depending standard configuration when it is installed. You can change this initial polling interval using the /poll-fast <fast> parameter (this is not recommended).

The /disc parameter can be specified to force the device to close the http sessions used immediately.

When the maintenance command file is retrieved, the commands found in the file are executed in sequence. Theoretically, all commands which can be typed in to a telnet session to the device or which appear in a config file can be used in the maintenance file. However, in most cases, you will use config change commands and commands to the UP0/UP1 modules.

The command file is executed every time it is retrieved (depending on the poll interval). However, in most cases, you don't want it to be executed each time, but only once. For example, if you are about to deploy a certain configuration change to all IPBSs, then you want this change to be done once per IPBS only. This can be achieved by the check command:

```
mod cmd UP1 check <final-command> <serial>
```

The devices maintain an internal variable UPDATE/CHECK which is initially (or when the device is reset to factory settings) empty. The check command will compare the <serial> parameter with the UPDATE/CHECK variable. If it is equal, any further processing of the command file is cancelled.

If it differs, the remainder of the file will be processed and, after the last command is executed, the UPDATE/CHECK variable will be set to <serial> and the <final-command> will be executed. The following commands are useful values for <final-command>:

ireset	resets the device as soon it is idle
reset	resets the device immediately
iresetn	resets the device as soon it is idle, only if a reset is required
resetn	resets the device immediately, only if a reset is required
ser	this is a no-op

Often, configuration changes shall be made only during certain times (e.g. non-working hours). This can be achieved using the times command:

```
mod cmd UP1 times [/allow <hours>] [/initial <minutes>]
```

The times command will check the current time against <hours>. If it does not match this restriction, any further processing of the command file is cancelled. <hours> is a comma separated list of hours. Only those hours listed are considered valid times for execution of the command file.

```
mod cmd UP1 times /allow 12,23,1,2,3,4
```

The command above allows command executions only between 12:00 and 12:59 and 23:00 and 4:59 local time (on a 24h clock). Note that if the device has no time set, all command executions will be cancelled.

If the /initial parameter is set, the no commands will be executed within the first <minutes> minutes after the device has been booted. This is done to avoid firmware download and flashing when installing devices.

```
mod cmd UP1 times /allow 12,23,1,2,3,4 /initial 6
```

The command above suppresses any command file processing within the first six minutes after each boot of the device. If /initial is set, new devices (or those that have been reset to factory settings), the command file will be retrieved even if it normally would be suppressed by the /allow parameter. This allows new devices to retrieve a site specific standard configuration quickly.

A.1.5 Setting the UP0 Parameters

To perform a firmware update, use the following command:

```
mod cmd UP0 prot <url> <final-command> <build-serial>
```

The command above downloads the new firmware from <url> and flash it to the device, then <final-command> is executed.

The IPBSs maintain an internal variable UPDATE/PROT which is initially (or when the device is reset to factory settings) empty. The prot command will compare the <build-serial> parameter with the UPDATE/PROT variable. If it is equal, no firmware will be loaded or flashed. If there is no UPDATE/PROT yet (like for a new device), <build-serial> is compared against the build number of the current firmware. After a successful download, UPDATE/PROT is set to <build-serial>. Note that <build-serial> is not checked against the firmware version actually loaded. It is your responsibility to keep this consistent.

If <url> ends with a slash ('/'), then a default firmware filename is added to the URL depending on the type of the device.

	Firmware filename
IPBS1	ipbs.bin
IPBS2	ipbs2.bin
IPBL	ipbl.bin

```
mod cmd UP0 prot http://192.168.0.10/firm/ ireset 5.0.0
```

The command above determines if firmware 5.0.0 is already installed. If not, new firmware will be downloaded from the following location depending on type of device:
IPBS1: http://192.168.0.10/firm/ipbs.bin
IPBS2: http://192.168.0.10/firm/ipbs2.bin
IPBL: http://192.168.0.10/firm/ipbl.bin
The UPDATE/PROT variable will be set to 5.0.0 and the device will be reset as soon as it is idle.

Similar to the prot command, the boot command will update the boot code.

	Boot filename
IPBS1	boot_ipbs.bin
IPBS2	boot_ipbs2.bin
IPBL	boot_ipbl.bin

```
mod cmd UP0 boot http://192.168.0.10/firm ireset 5.0.0
```

The command above determines if boot code 5.0.0 is already installed. If not, new boot code will be downloaded from the following location depending on type of device:
IPBS1: http://192.168.0.10/firm/boot_ipbs.bin
IPBS2: http://192.168.0.10/firm/boot_ipbs2.bin
IPBL: http://192.168.0.10/firm/boot_ipbl.bin
The UPDATE/BOOT variable will be set to 5.0.0 and the device will be reset as soon as it is idle.

Using UP0, device configurations can be saved to a web server.

```
mod cmd UP0 scfg <url>
```

This will cause the device to upload its current config to url This will be done using an HTTP PUT command. url must be writable thus. With url, some meta character strings are replaces as follows:

Sequence	**Replacement**	**Example**
#d	Current date and time	20040319-162544
#m	Device mac address	00-90-33-03-0d-f0
#h	Device hardware ID	ipbs-03-0d-f0
#b	Rolling backup index loops over 0 .. n-1 for each backup	5

A.1.6 Setting the RFP_UPDATE0 Parameter

To perform a RFP firmware update, use the following commands.

```
mod cmd RFP_UPDATE0 firmware http://192.168.0.10/
Worf4_GAP_R4H.s2
```

The command above specifies the url to the RFP firmware to use.

```
mod cmd RFP_UPDATE0 select 0x2753
```

Specifies which RFPs to update using a hex-encoded bit-mask. Each bit represents an RFP port starting with port 1 at the LSB (0x0001) up to port 16 (0x8000).

0x2753 specifies RFP "1,2,5,7,9,10,11,14" to be updated.

```
mod cmd RFP_UPDATE0 schedule DD.MM.YYYY-HH:MM
```

Specifies when the update shall start. If no date is provided, the update will be immediate when the start command is issued.

```
mod cmd RFP_UPDATE0 start /idle
```

Starts the update or activates the schedule. Normally the /idle command is selected and an update starts only if the RFP is idle.

If multiple RFPs are selected for update, they will be updated one at a time If /sequence command is used.

Example Update RFP Firmware

This example shows an "update file" for the IPBL.

```
mod cmd UP1 check ser 20070316-1

mod cmd RFP_UPDATE0 firmware http://172.20.8.125/ascom/rfp/
Worf123.S2

mod cmd RFP_UPDATE0 select 0xffff

mod cmd RFP_UPDATE0 start /idle
```

Example IPBS1/IPBS2/IPBL Boot and Firmware Update

This example shows an "update file" for the IPBS1/IPBS2 and IPBL.

```
mod cmd UP0 prot http://172.20.8.128/ascom/firmware/ ireset
5.0.0

mod cmd UP0 boot http://172.20.8.128/ascom/boot/ ireset 5.0.0
```

A.1.7 Configuration File Backup

To make a backup of the configuration file, use the following command:

```
mod cmd UP0 scfg <url> [<final-command> <save-serial> [ /force
<hours>]]
```

The scfg command uploads the current configuration file to the specified <url>.

Example

```
mod cmd UP0 scfg http://192.168.0.10/configs/saved/#h#b5.txt no-
op WEEKLY /force 168
```

The command above saves the device configuration file once a week with a backlog of 5 weeks.

To load a configuration file on the IP-DECT device use the following command:

```
mod cmd UP0 cfg <url> <final-command> <serial>
```

The command loads the configuration file, and all commands in it are executed.

Appendix B: RFP Power Consumption

The tables below show power consumption for a base station connected to and powered from the IPBL. The power consumption of the IPBL is approximately 15 W.

The maximum cable length for base stations connected to the IPBL must **not** exceed 1500 meters.

B.1 KRCNB 201/DCT1800

Cable length (metres)	0.4 mm wire size (∅)		0.5 mm wire size (∅)		0.6 mm wire size (∅)	
	Without EPP	With EPP	Without EPP	With EPP	Without EPP	With EPP
0	7.5	7.5	7.5	7.5	7.5	7.5
100	7.9	7.8	7.8	7.7	7.7	7.6
200	8.3	8.0	8.0	7.8	7.8	7.7
300	8.9	8.3	8.3	8.0	8.0	7.8
400	9.8	8.7	8.7	8.2	8.2	7.9
500	11.3	9.2	9.2	8.5	8.4	8.0
600	-	9.8	9.8	8.7	8.6	8.2
700	-	10.7	10.7	9.0	8.8	8.3
800	-	12.3	12.3	9.4	9.1	8.4
900	-	-	-	9.8	9.5	8.6
1000	-	-	-	10.3	9.9	8.8
1100	-	-	-	11.1	10.4	8.9
1200	-	-	-	12.3	11.1	9.1
1300	-	-	-	-	12.1	9.3
1400	-	-	-	-	-	9.6
1500	-	-	-	-	-	9.9

Table 1 Power consumption (watts) of base stations and cabling when powered from the IPBL.

B.2 BS3x0 and DB1

Cable length (metres)	0.4 mm wire size (∅)		0.5 mm wire size (∅)		0.6 mm wire size (∅)	
	Without EPP	With EPP	Without EPP	With EPP	Without EPP	With EPP
0	5.0	5.0	5.0	5.0	5.0	5.0
100	5.2	5.1	5.1	5.1	5.1	5.1
200	5.3	5.2	5.2	5.1	5.1	5.1
300	5.6	5.3	5.3	5.2	5.2	5.1
400	5.8	5.5	5.5	5.3	5.3	5.2
500	6.1	5.6	5.6	5.4	5.4	5.2
600	6.5	5.8	5.8	5.5	5.4	5.3
700	7.1	6.0	6.0	5.6	5.5	5.3
800	8.1	6.2	6.2	5.7	5.6	5.4
900	-	6.5	6.5	5.8	5.7	5.4
1000	-	6.9	6.9	5.9	5.8	5.5
1100	-	7.3	7.3	6.1	5.9	5.6
1200	-	8.1	8.1	6.2	6.1	5.6
1300	-	-	-	6.4	6.2	5.7
1400	-	-	-	6.6	6.4	5.8
1500	-	-	-	6.9	6.6	5.8

Table 2 Power consumption (watts) of base stations and cabling when powered from the IPBL

Appendix C: Local R-Key Handling

Local R-key handling assume that the check box for local R-key handling is selected, see 8.5.8 *Local R-Key Handling* on page 91.

The following R-key functions are available during a call.

Key	Description
R	Put the ongoing call on hold and get a new line. (Dial the number to the second call.)
R0	Send busy signal to the incoming call.
R1	Terminate the ongoing call and switch to call on hold/incomming call.
R2	Switch between ongoing call and call on hold/incomming call.
R3	This function (normally used for three-party conference) is not supported in the IP-DECT System.
R4	Transfer call on hold to ongoing call and disconnect.
RR (unattended transfer)	Put the ongoing call on hold and dial the number to the destination where the last held call shall be transferred to.

Appendix D: Database Maintenance

This section describes how IP-DECT user configuration can be moved from one system to another. By moving users, one IP-DECT system can be split into many systems or several IP-DECT systems can be merged to one single system.

Before database merge you should consider if the IP-DECT R3 Multi Master concept can be used instead and whether it is possible to have several Masters on one site.

D.1 Prerequisites

For all systems involved in the database maintenance procedure:

- It is highly recommended to have the same software version running on all systems.
- If a user is moved to a system with a different SARI, the target system must be configured with multiple SARIs containing the SARI number of the originating system as well as its existing SARI. For more information, see 8.5.26 *SARI* on page 100.
- The systems must have the same DECT system name and the same DECT system password (configured under DECT > System) as well as the same device password (General > Admin).
- LDAP replication must not be activated.

D.2 Database Maintenance Procedure

1 Make sure the handsets that correspond to the moved user data have no contact with the system. Turn off the handsets or switch off the Radio(s) in the area where the handsets are located. Handsets should show "No system". Handsets may be desubscribed if they have connection to the system during database maintenance.

2 Save a configuration file from each Master involved. See 8.14 *Backup* on page 126.

3 Identify user records in the saved configuration files and modify them according to the desired plan. User records are located at the end of the file beginning after the row:

```
mod cmd FLASHDIR0 add-view 101 cn=PBX0
```

4 To remove a user, remove the corresponding line.

To add a user (from another file), insert a line that has been removed from another file. Remove the following attributes:

```
(guid;bin=###)
```

```
(usn=###)
```

where ### denotes an arbitrary value.

5 Save modifications to the configuration files.

6 Make sure that step 1 is met, and upload configuration files to the corresponding entities. See 8.18.1 *Update Configuration* on page 130.

7 Reset in order to make the changes take effect, see 8.22 *Reset* on page 138.

Removing a User Example

This example shows part of the configuration file. There may also be other attributes in the used system.

Before Removal

```
mod cmd FLASHDIR0 add-view 101 cn=PBX0
mod cmd FLASHDIR0 add-item 101
(cn=1950)(guid;bin=80319FC0E909D311905C00013E00EFC8)(dn=
1950)(h323=1950)(e164=1950)(pbx=<user admin="no"/
>)(pbx=<gw name="DECT_CEg" ipei="002020173394"
subs="977e9bfc568c8223197e4195bec9ec28"/>)(usn=14)
mod cmd FLASHDIR0 add-item 101
(cn=1951)(guid;bin=7B7C9D01E909D311905C00013E00EFC8)(dn=
1951)(h323=1951)(e164=1951)(pbx=<user admin="no"/
>)(pbx=<gw name="DECT_CEg" ipei="002020173479"
subs="90bd79116daec066105610822cabc1e7"/>)(usn=15)
```

After Removal

```
mod cmd FLASHDIR0 add-view 101 cn=PBX0
mod cmd FLASHDIR0 add-item 101
(cn=1950)(guid;bin=80319FC0E909D311905C00013E00EFC8)(dn=
1950)(h323=1950)(e164=1950)(pbx=<user admin="no"/
>)(pbx=<gw name="DECT_CEg" ipei="002020173394"
subs="977e9bfc568c8223197e4195bec9ec28"/>)(usn=14)
```

Adding a User Example

This example shows part of the configuration file. There may also be other attributes in the used system.

Before Addition

```
mod cmd FLASHDIR0 add-view 101 cn=PBX0
mod cmd FLASHDIR0 add-item 101
(cn=1950)(guid;bin=80319FC0E909D311905C00013E00EFC8)(dn=
1950)(h323=1950)(e164=1950)(pbx=<user admin="no"/
>)(pbx=<gw name="DECT_CEg" ipei="002020173394"
subs="977e9bfc568c8223197e4195bec9ec28"/>)(usn=14)
```

After Addition

```
mod cmd FLASHDIR0 add-view 101 cn=PBX0
mod cmd FLASHDIR0 add-item 101
(cn=1950)(guid;bin=80319FC0E909D311905C00013E00EFC8)(dn=
1950)(h323=1950)(e164=1950)(pbx=<user admin="no"/
>)(pbx=<gw name="DECT_CEg" ipei="002020173394"
subs="977e9bfc568c8223197e4195bec9ec28"/>)(usn=14)
mod cmd FLASHDIR0 add-item 101
(cn=1951) (dn=1951)(h323=1951)(e164=1951)(pbx=<user
admin="no"/>)(pbx=<gw name="DECT_CEg"
ipei="002020173479"
subs="90bd79116daec066105610822cabc1e7"/>)
```

The `guid;bin` and `usn` attributes are not insterted. The system will create these attributes when the file is uploaded to the device.

Appendix E: Load Balancing

Load balancing can be used in an IP-DECT system when the number of handsets exceeds what an IP-PBX is able to register.

When load balancing the traffic is distributed over several IP-PBXs which can be done in two ways using:

- fixed connections for users on each Master towards *multiple* IP-PBXs.
- dynamic connection for users on each Master towards IP-PBX *network* using DNS services.

E.1 Load Balancing Using Fixed Connection Towards IP-PBXs

When the number of users exceeds what an IP-PBX is able to register, you can load balance using several IP-PBXs where each Master in the IP-DECT system is connected to a fixed IP-PBX.

Note: For redundancy, an alternative gatekeeper/proxy should always be used.

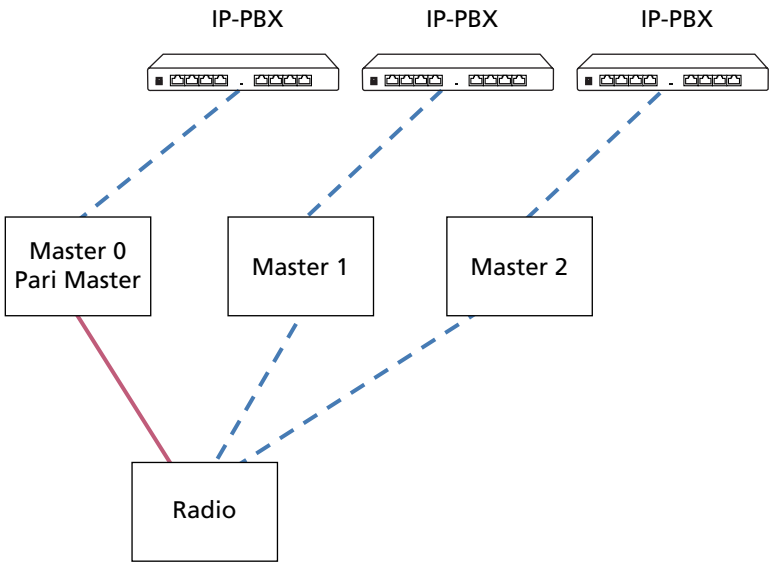


Figure 1. Load balancing using fixed connection towards IP-PBXs.

1 Select DECT > Master.

2 In the drop-down list, select "SIP" protocol.

3 Enter the IP address or host name and optionally port of proxy (e.g. proxy1.ascom-rd.com:5060) to the SIP proxy (registrar) in the Proxy text field.

4 To get redundancy: Enter the IP address or host name and optionally port of proxy (e.g. proxy2.ascom-rd.com:5060) to the alternative SIP proxy (registrar) in the Alt. Proxy text field.

5 Reset in order to make the changes take effect, see *8.22 Reset*.

E.2 Load Balancing Using Dynamic Connection Towards IP-PBX Network

When the number of users exceeds what an IP-PBX is able to register, you can use load balancing towards an IP-PBX network. Using DNS services, users on each Master are

dynamically connected towards the IP-PBX network. In addition to the load balancing of the traffic, redundancy is also achivied.

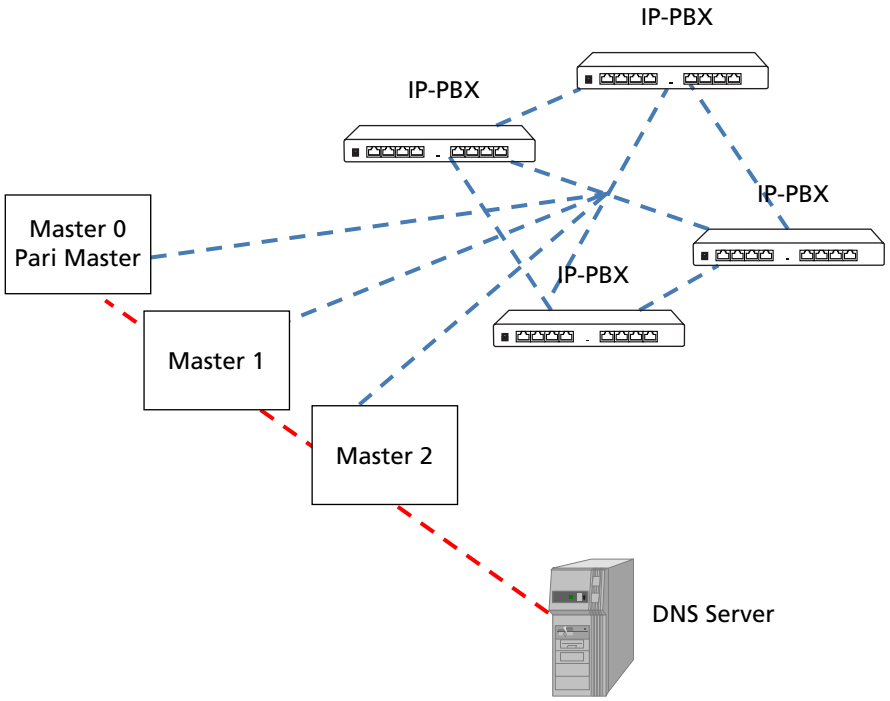


Figure 2. Load balancing using dynamic connection towards IP-PBX network.

E.2.1 How the Load Balancing Works

When you register a handset, a SRV-type query is sent to the DNS server asking for existing SIP proxys (IP-PBXs) in the domain defined in the Master. The DNS server will reply with a list of SRV (Service) records, one for each IP-PBX. Each SRV record contains a priority and a weight value. Lower priority value means more preferred. When there are two or more records with the same priority, then the weight value determines which IP-PBX the user should be dynamically connected to.

A DNS server assign each user a primary and a secondary proxy address using DNS-SRV service mechanism.

E.2.2 Local Site Redundancy

If redundancy is wanted in a remote site, that is you want to be able to make emergency phone call if the WAN connection to the central site goes down, a local site proxy server, e.g. SRST (Cisco), can be used in the remote site, see figure 3 on page 160.

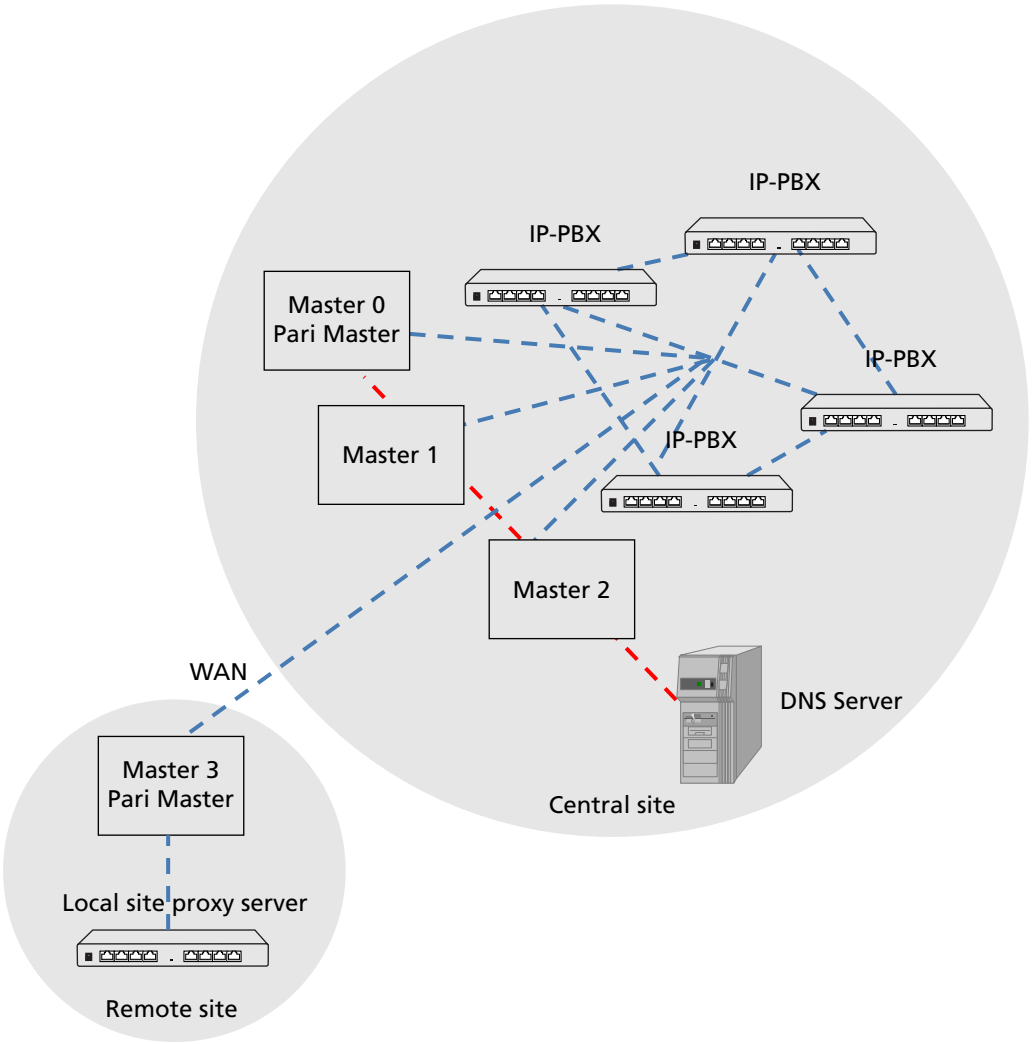


Figure 3. Redundancy in the remote site using a local site proxy server.

E.2.3 About SRV Records

Record format

An SRV record has the form:.

```
_Service._Proto.Name TTL Class SRV Priority Weight Port Target
```

- **Service**: the symbolic name of the desired service.
- **Proto**: the protocol of the desired service; this is usually either TCP or UDP.
- **Name**: the domain name for which this record is valid.
- **TTL**: standard DNS time to live field.
- **Class**: standard DNS class field (this is always IN).
- **Priority**: the priority of the target host, lower value means more preferred.
- **Weight**: A relative weight for records with the same priority.
- **Port**: the TCP or UDP port on which the service is to be found.
- **Target**: the hostname of the machine providing the service.

An example of an SRV record might look like this:

```
_sip._udp.ascom-rd.com. 86400 IN SRV 0 5 5060 sipserver.ascom-rd.com.
```

This points to a server named sipserver.ascom-rd.com listening on TCP port 5060 for SIP protocol connections. The priority given here is 0, and the weight is 5.

SRV records must contain the fully qualified domain name (FQDN) of the host.

How to set priority and weight

SIP clients always use the SRV record with the lowest-numbered priority value first, and only fall back to other records if the connection with this record's host fails. Thus a service may have a designated "fallback" server, which will only be used if the primary server fails. Only another SRV record, with a priority field value higher than the primary server's record, is needed.

If a service has multiple SRV records with the same priority value, clients use the weight field to determine which host to use. The weight value is relevant only in relation to other weight values for the service, and only among records with the same priority value.

In the following example showing five records, both the priority and weight fields are used to provide a combination of load balancing and backup service.

```
_sip._udp.ascom-rd.com. 86400 IN SRV 10 60 5060 bigbox.ascom-rd.com.
_sip._udp.ascom-rd.com. 86400 IN SRV 10 20 5060 smallbox1.ascom-rd.com.
_sip._udp.ascom-rd.com. 86400 IN SRV 10 20 5060 smallbox2.ascom-rd.com.
_sip._udp.ascom-rd.com. 86400 IN SRV 20 50 5060 backupbox1.ascom-rd.com.
_sip._udp.ascom-rd.com. 86400 IN SRV 20 50 5060 backupbox2.ascom-rd.com.
```

The first three records with priority 10 are primary servers and the last two records with priority 20 are secondary servers.

For each client, a primary server is selected at random with the help of the weight values 60, 20 and 20. This will distribute all clients on the primary servers according to the weight values.

If a client's primary server goes down, the client will use the secondary server instead, i.e. **backupbox1.**ascom-**rd.com** and **backupbox2.**ascom-**rd.com.**

E.2.4 Load Balancing Using Dynamic Connection: Master Settings

1 Select DECT > Master.

2 In the drop-down list, select "SIP" protocol.

3 Enter the SIP server's domain address.

4 A local site proxy server (IP-PBX), e.g. SRST (Cisco), can be used to make emergency phone call in case that the WAN connection goes down, see E.2.2 *Local Site Redundancy* on page 159.
Enter the IP address or host name and optionally port of proxy (e.g. proxy2.ascom-rd.com:5060) to the local site proxy server in the Alt. Proxy text field.

5 Reset in order to make the changes take effect, see *8.22 Reset*.

6 Repeat step 1 to 5 for all exisiting Masters.

E.2.5 Load Balancing Using Dynamic Connection: DNS Server Settings

The example below shows the settings in Microsoft Windows Server where the DNS server is installed.

1 From a Microsoft Windows Server with the DNS server installed, open the DNS management tool.

2 Right click the domain (or subdomain) you are assigning this service to and select "Other New Records...".

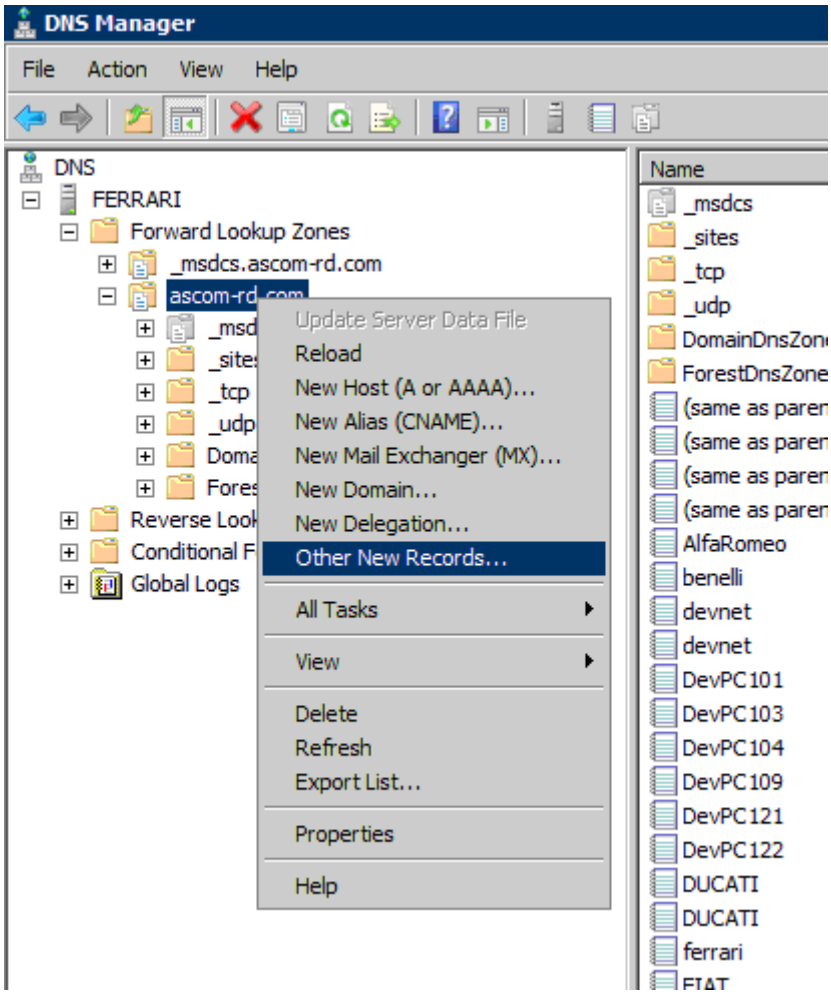


Figure 4. Select "Other New Records...".

3 Scroll down to Service Location (SRV) in the list.

4 In the "New Resource Record" window, see Figure 5, do as follows:

Enter "_sip" in the *Service* field.

Enter _udp in the *Protocol* field.

Assign a priority and weight. For information on how to set priority and weight, see E.2.3 *About SRV Records* on page 160.

Enter "5060" as the port number.

Enter the host name of your SIP server (IP-PBX). Note: The host name must be a fully qualified domain name (FQDN).

Click "OK".

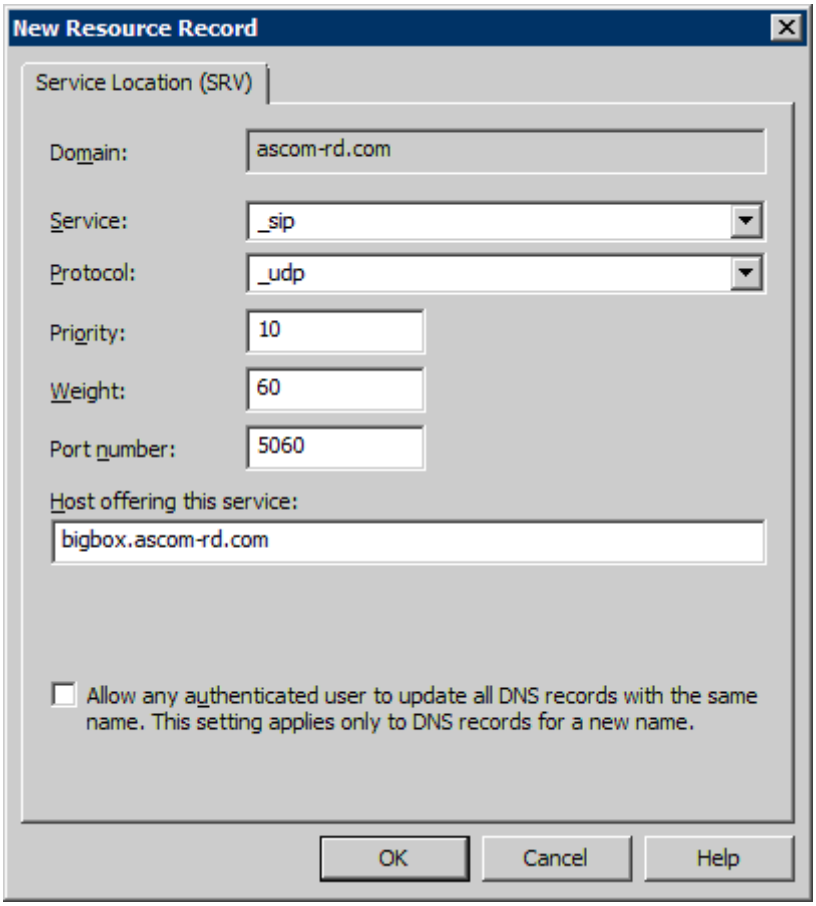


Figure 5. New resource record settings

5 You can view your new SRV record by clicking on the _udp item under your domain.

6 Right click the domain (or subdomain) where the new SRV record is located and select "New Host (A)...".

7 In the "New Host" window, see Figure 6, do as follows:

Enter in the *Name* field the host name of your SIP server (IP-PBX).

Verify that the fully qualified domain name (FQDN) is the correct one.

Enter the IP address of your SIP server.

Click "Add Host".

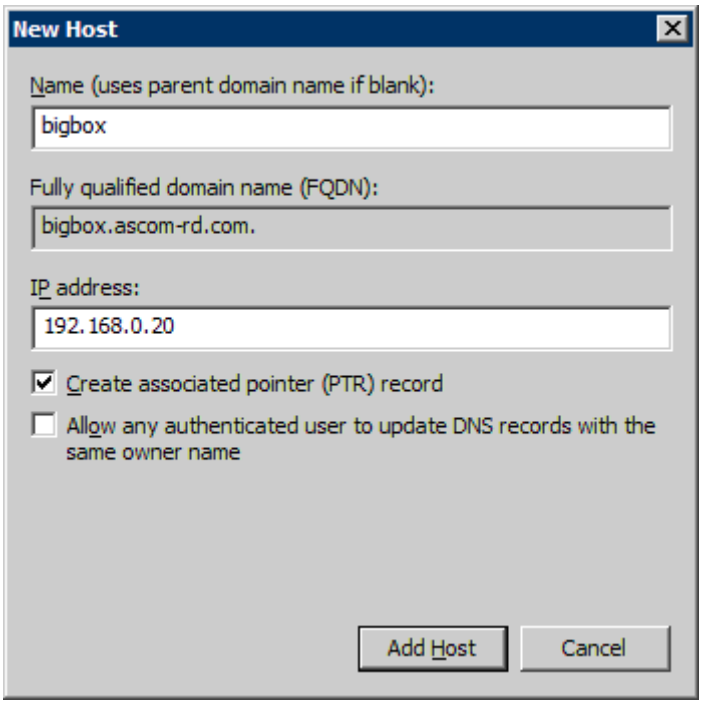


Figure 6. New host settings

8 Repeat step 1 to 7 for all exisiting IP-PBXs.

Appendix F: Update Script for Configuration of Kerberos Clients

The update script is as follows:

```
mod cmd UP1 check resetn serial002

config add NTP0 /addr 192.168.42.136

vars create CMD0/KCMD p
<join+realm="negrealm1"+user="neguser1"+password="negpwd1"+
force="true"+disable-local="true"><server+realm="negrealm1"+
address="192.168.42.34"/><server+realm="negrealm2"+address=
"192.168.42.99"/></join>
```

Description of the update script:

Command line 1: `mod cmd UP1 check resetn serial002`

By inserting this into the update script file the update server will check the variable ''check'' and if the value (serial002) is different from the value in the update server this script will be executed and the box will be rebooted afterwards.

Command line 2: `config add NTP0 /addr 192.168.42.136`

By inserting this into the update script the local Time server is configured with IP address to valid time server and active time can be retrieved. Correct time is very important in Kerberos for joining of realm and for login purpose.

Command line 3: `vars create CMD0/KCMD p ....`

The format of this line is very important. It is very important to only modify the data surrounded with double quote (''''). This script describes the mandatory data, the other data is set to default values. All parameters set by the Add-tab (see section 1) is possible to set with this script.

The XML format is as follows:

```
<join realm="..." host="..." user="..." password="..." disable-
local="..." force="..."><server realm="..." address="..." port="..."
secondary-address="..." secondary-port="..."/></join realm>
```

`realm`: The realm to join
`host`: The host name for the box (optional, otherwise the hardware id will be used)
`user`: Admin user name from the Kerberos server
`password`: Admin password from the Kerberos server
`disable-local`: the config flag will be set accordingly (true or false, optional, defaulting to false)
`force`: tells if an existing realm membership shall be discarded (true or false, optional, defaulting to false)
`server`: multiple servers may be given

In the above example two servers are configured one for the Kerberos server and one if using an or Standby Kerberos server.

Appendix G: Install Certificate in the Web Browser

To access the GUI for an IPBS/IPBL using secure web access (https), the certificate for the IPBS/IPBL can be installed in the web browser to avoid getting certificate error messages.

To install the certificate, perform the following two steps:

Step 1. Create a certificate. See *G.1 Create a Certificate*.

Step 2. Install the certificate in the web browser. See *G.2 Install the Certificate*.

G.1 Create a Certificate

Note: Make sure the name you use to access the IPBS/IPBL is in the "Common Name" of the certificate (e.g. IP-address) or if the name is an FQDN, in the "DNS Name". The Web Browser will require a match when validating the certificate information.

Create a certificate by selecting one of the following two types of certificate handling options:

- Self-signed certificate
  This option is for customers not planning on having their certificates signed by public or private CAs. Self-signed certificates provide encryption but do in most cases not provide authentication. For more information see *Self-signed Certificates* on page 76.

- Certificates signed by a Certificate Authority (CA)
  Two options are possible:
  A Certificates signed by the customer's own CA. Customers possessing the knowledge and infrastructure to house their own CA could build an internal enterprise CA, enabling them to sign (approve) their own certificate requests. This would make the customer a private CA.
  B Certificates signed by a trusted public third party entity/organization. There are only about a dozen issuers who have the authority to sign certificates for servers worldwide. An example is VeriSign. To use a public CA for certificate approvals the IP-DECT system would in most cases need to be connected to the Internet and hold a fully qualified domain name. For more information see *Certificate Signing Request (CSR)* on page 77.

G.2 Install the Certificate

The instructions below apply for Internet Explorer version 8 and may differ for later versions.

Note: If your PC is running Windows Vista or later, select "run as administrator" for Internet Explorer.

1 Access the GUI for an IPBS/IPBL. A security warning window will appear when using secure web access (https) to access the GUI.

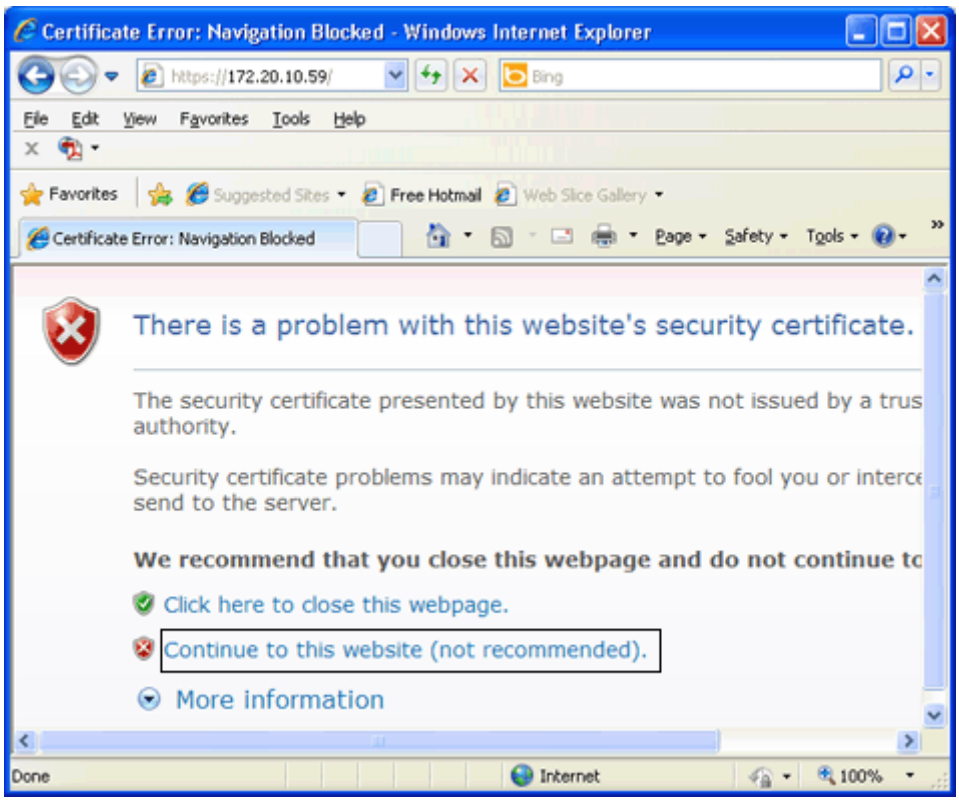

Certificate Error: Navigation Blocked - Windows Internet Explorer
https://172.20.10.59/
Bing
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Free Hotmail
Web Slice Gallery
Certificate Error: Navigation Blocked
Page
Safety
Tools
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trus
authority.
Security certificate problems may indicate an attempt to fool you or interce
send to the server.
We recommend that you close this webpage and do not continue to
Click here to close this webpage.
Continue to this website (not recommended).
More information
Done
Internet
100%

Figure 7. Security warning window.

2 In the security warning window, click on the text link "Continue to this website (not recommended)." The login window for the device will appear.

3 Click on the "Certificate Error" notification in the Security Status bar (next to the Internet Explorer Address bar), see Figure 8. The Security Report window will

appear, see Figure 9.

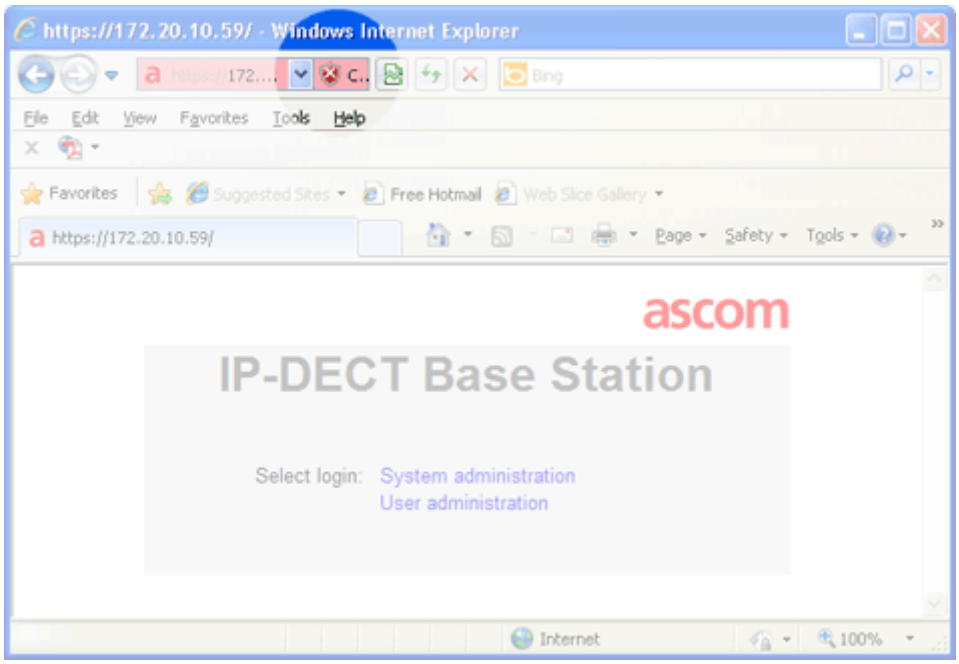


Figure 8. Sceen shot of the login window, with the "Security Status bar highlighted.

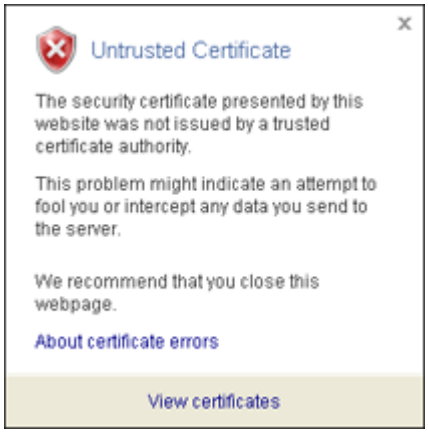

Untrusted Certificate
The security certificate presented by this website was not issued by a trusted certificate authority.
This problem might indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage.
About certificate errors
View certificates

Figure 9. The Security Report window.

4 In the Security Report window, click on the blue text link "View certificates". The Certificate window will appear.

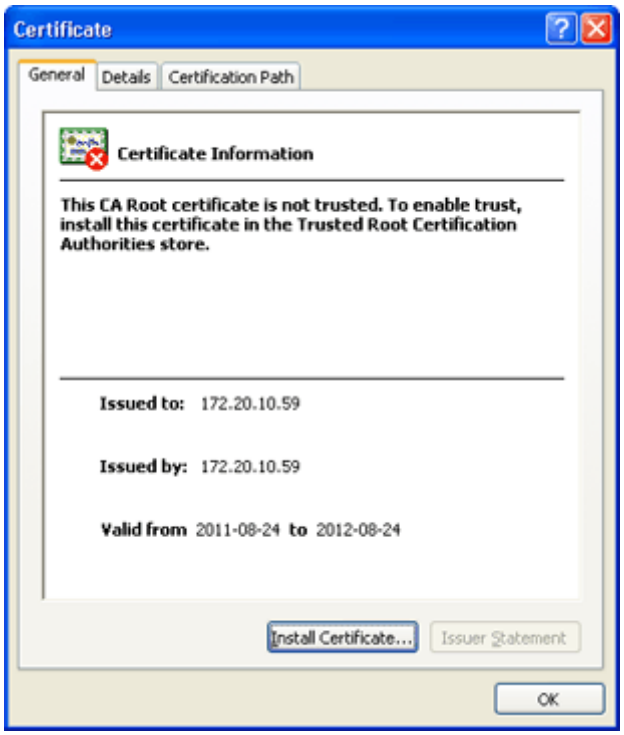


Figure 10. The Certificate window.

5 In the Certificate window, click on the button "Install Certificate...". The Certificate Import wizard is started.

6 Click on "Next".

7 Make sure that option "Automatically slelct the certificate store based on the type of certificate" is selected, see Figure 11. Click on "Next".

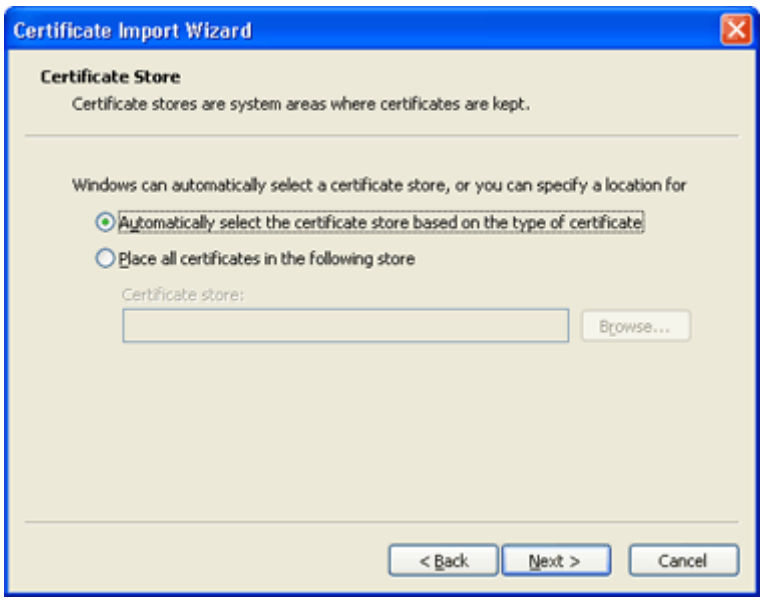

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
< Back
Next >
Cancel

Figure 11. The Certificate Import wizard.

8 Click on "Finish" to complete the Certificate Import wizard. The Security Warning window will appear.

9 Click on "Yes" to install the certificate".